International Conference on Nuclear Security 2020

Report of Contributions
Ghana’s Nuclear Security: progress, challenges, and the way forward

This work assesses Ghana’s Nuclear Security Regime in the wake of sustained upsurge in the frequency of activities of extremist groups in the west African sub region, highlights the key challenges Ghana is facing in implementing its Nuclear Security regime, and recommends a number of next steps for a forward outlook. The formation of the Nuclear Regulatory Authority, Physical Protection upgrades in facilities and sustained cooperation with both local and international stakeholders in nuclear security like the Bureau of National Investigation, Immigration Services, Custom Excise and Preventive Services, Ghana Police Service, Ghana Armed Forces and the IAEA, The United States Department of Energy’s National Nuclear Security Administration (NNSA) Office of Radiological Security (ORS), the Lawrence Livermore National Laboratory, ROSATOM and Government of China were found to be major progress made in advancing Nuclear Security in Ghana. Some challenges identified included the delay in the formulation of regulations for nuclear security by the regulator and the lack of realistic force on forces exercises the test the adequacies of the systems provided for security. On the way; forwards the paper proposes some actions including: conducting of a force on force exercise involving all major stake holders, the development of a National DBT based on which facilities could develop their DBT for security implementation and improving security culture through trainings and assessments and improving and expanding the activities of the Nuclear Security Support Centre into a Centre of Excellence for Nuclear Security in the region.

State
Ghana

Gender

Primary author: Mr AGALGA, Raymond (Ghana Atomic Energy Commission)

Co-authors: Mr ATTAH AMOAH, Paul (Ghana Atomic Energy Commission); Mr ADJEI, Daniel Nii (Ghana Atomic Energy Commission); Mr FREDERICK CHARLES, Daniel (Ghana Atomic Energy Commission)

Presenters: Mr AGALGA, Raymond (Ghana Atomic Energy Commission); Mr ATTAH AMOAH, Paul (Ghana Atomic Energy Commission)

Track Classification: CC: Use of IAEA and other international guidelines for building national nuclear security regimes
International Transport of Nuclear Material in Brazil – a model of success

The purpose of this work is to demonstrate how International Transport of Nuclear Material in Brazil is organized, coordinated and executed according to the National Nuclear Security Regime. The country has established a Nuclear Security governance in the President of the Republic Institutional Security Cabinet which has a central role in the System for the Protection of the Brazilian Nuclear Program (Sipron), with the recent implementation of the Nuclear Security Coordination in its structure. This new organization enabled the coordination of all national assets involved in the security of nuclear material during transport. Brazil has extensive dimensions, it occupies roughly half of South America, bordering the Atlantic Ocean and all the subcontinent countries except Ecuador and Chile. This continental country presents huge challenges to the ground transportation of any kind in order to reach neighboring countries. Nevertheless, in 2018, a successful nuclear material transport operation to Argentina was coordinated by Sipron within a length of more than 2,000 Km. Nuclear material was delivered from Resende in the State of Rio de Janeiro to Uruguaiana in the State of Rio Grande do Sul in the border with Argentina. This represents an itinerary farther then the distance between Vienna and Moscow. The Coordination of Nuclear Security carried out various activities before and during the operation. First of all these activities were concerned to the identification of all stakeholders roles and responsibilities with the purpose to achieve the necessary synergy in order to perform the operation jointly. The Design and Evaluation Process Outline (DEPO) methodology was applied and the following tasks were accomplished: transportation conveyance characterization; risk and threat assessment with the support of the national intelligence agency; physical protection design according to a defined threat; law enforcement coordination (Federal Police and State Polices); contingency planning; information security measures; personnel clearances; coordination with highway operators; regulatory compliance; activation of the National Command and Control Joint Center and the State Command and Control Joint Centers; synchronization matrix implementation. The operation proved the importance of liaison in all levels, information sharing and cooperation among the responders. However the principle of confidentiality application became crucial to restrict access to sensitive information to the minimum necessary. Deterrence was largely employed during the operation to minimize risks. The operation has turned into a successful interagency Case Study with many Best Practices and Lessons Learned.

Key Words: Nuclear security regime; nuclear material transport, joint interagency operation.

State

Brazil

Gender

Male

Primary authors: Mr ROMAO, Cesar (Brazilian Government - Institutional Security Cabinet); Mr PETRUCELI, Fabiano (Brazilian Government - Institutional Security Cabinet)

Presenters: Mr ROMAO, Cesar (Brazilian Government - Institutional Security Cabinet); Mr PETRUCELI, Fabiano (Brazilian Government - Institutional Security Cabinet)
Track Classification:  PP: Transport of nuclear and other radioactive material: practices, challenges and regulatory issues
FIRST NATIONAL EXERCISE IN COMPUTER SECURITY IN NUCLEAR SECTOR IN SLOVENIA

Whether we like it or not, acknowledge it or not, the number of cyber-attacks is increasing. Malicious actors are continuously becoming more sophisticated, highly motivated, some also well-funded, and focused on the nuclear sector. If cyber-attacks in the nuclear sector were to be successful, consequences of such an attack could potentially be catastrophic for people and the environment. Therefore, our efforts in computer security must increase. One example is conducting computer security exercises, which are an essential element in assuring a high level of computer security supporting nuclear security. The main objectives of exercises are awareness, testing internal procedures, identifying gaps in computer security measures, testing the efficiency of computer security plans and response arrangements, training the Computer Security Incident Response Team, etc. All of these objectives, and more, can be achieved by different types of exercises: table-top, drills, blue vs red, simulated and combined exercises, etc. To our knowledge, there were only a handful of computer security exercises conducted in the nuclear sector to date. In order to substantiate our beliefs, we conducted research, comprised of descriptive analysis of various publicly available sources, structured interviews with national and international experts in nuclear sector and verified our findings with emergency preparedness experts, employed at the Slovenian Nuclear Safety Administration. The results of our research represent a structured and comprehensive approach in preparation, conduct and evaluation of computer security exercises. Based on the results of the research, the first national exercise in computer security in nuclear sector in Slovenia called KIVA2019 was prepared. The exercise was conducted in January 2019 as a one-day table-top exercise with a short storyline and a cyber-attack scenario based on current computer security incidents in critical infrastructure. Exercise was attended by participants from all key national stakeholders in the nuclear sector: nuclear facility operators, competent authorities, technical support organizations and suppliers of computer software and hardware equipment. Due to the importance of this topic on a national level, the exercise was attended also by external observers from the Slovenian Ministry of Interior, Ministry of Public Administration and Faculty of Criminal Justice and Security. Evaluation of the exercise comprised of detailed analysis and an action plan, including further steps that are needed to fill in the gaps identified during the exercise. These gaps are not new to nuclear security and generally include the improvement of information sharing on a national and international level and harmonization of response arrangements for cyber-attacks by all key stakeholders in nuclear sector. Additionally, KIVA2019 represents a starting point for future computer security exercises in Slovenia. Knowledge gained from this research and KIVA2019 will contribute to the preparation of future exercises, enhance cooperation between key stakeholders, and thus improve computer security and nuclear security in the Slovenian nuclear sector and in general.

State

Slovenia

Gender
Primary authors:  Mr TOMAZIC, Samo (Slovenian Nuclear Safety Administration); Dr BERNIK, Igor (Faculty of Criminal Justice and Security); Mrs TOMAZIC, Metka (Slovenian Nuclear Safety Administration)

Presenter:  Mr TOMAZIC, Samo (Slovenian Nuclear Safety Administration)

Track Classification:  CC: Good practices in the development and execution of nuclear security exercises (e.g. tabletop, drills and field exercises);
THE NUCLEAR SECURITY CONCERNS ON THE RECENTLY DEVELOPTED BRAZILIAN NATIONAL NUCLEAR POLICY

Inside of the Brazilian Republic Presidency, the National Security Cabinet is responsible for two important assignments: The coordination of the Brazilian Nuclear Program Protection System (Sipron), responsible for the actual Brazilian nuclear safety and security concerns, and the Brazilian Nuclear Program Development Committee (CDPNB), which is a multiministerial collegiate responsible for the future of the Brazilian nuclear sector. Among plenty of tasks, the Committee is up to proposing solutions on many issues and helping the development of our nuclear sector. The Brazilian nuclear sector, which began its activities in 1960, was still in the need of a National Policy to present the principles, guidelines and goals for the development of the sector. In this sense, a multiministerial technical group was created, within the scope of the CDPNB, to analyze the main strategic issues on our country and increase the synergy among the involved sectors. As a final product, a draft of the Brazilian National Nuclear Policy was presented and further on approved by the President that released it by a Decree, on December 5th, 2018. This Policy brought important progress by raising important themes involving nuclear safety and security and bringing them to the highest Brazilian Executive level. So many contributions started to appear pointing out solutions to current obstacles on the development of the Brazilian nuclear sector. The main principles defined on our National Nuclear Policy are: the use of nuclear technology for peaceful purposes; the observance of conventions, agreements and treaties; nuclear safety and security; the full knowledge of nuclear fuel cycle; the use of nuclear technology for national development and social welfare and directions to ambientals prevention. The main objectives of the Brazilian National Nuclear Policy are: to keep the knowledge about nuclear technology; to comply with national energy sector decisions, pointing to nuclear power generation; to ensure the safe use of nuclear technology; to strength the planning and the response to emergency situations and safety/security events; to promote society consciousness about the benefits and the safe use of nuclear technology; to reinforce Brazilian commitments on nuclear disarmament and non-proliferation; to update and keep the structure of the Brazilian Nuclear Sector, avoiding overlapping and conflicting tasks; to encourage research, development and innovation; to promote cooperation between ST&I Institutions, as well as with users; to foster research and exploration of nuclear ores; to boost the national production of nuclear ores and their byproducts; to guarantee the strategic geological resource and the strategic stock; to pursue autonomy on the production of nuclear fuel in industrial scale; to foster self-sufficiency in radioisotopes and their export; to promote professional training and to keep human resources on our nuclear sector; to encourage technical, scientific and industrial training; to foster planning and execution of projects, in order to optimize the use of human resources and to guarantee the safe management of radioactive waste.

The construction of the Brazilian National Nuclear Policy is a case of success on a multiministerial effort, by the Brazilian National Security Cabinet guidance. Could be interesting to share, on a presentation at the conference and exploring the theme "National nuclear security regimes", ours high level challenges and the actions made to mitigate them. Also share the International Atomic Energy Agency (IAEA) contribution to achieve the efficiency of Brazilian nuclear security and safety, by establishing comprehensive guidance and supporting us building technical capacity, including education and training. A National Nuclear Policy must be the first step on the evolution of a nuclear security regulation. Its promulgation can legitimizes and reinforce several and necessary
actions to be undertaken and allows to restructure the governance of a State nuclear sector.

**State**

Brazil

**Gender**

Male

**Primary authors:** Dr TAVEIRA, MARCIO (BRAZILIAN PRESIDENCY); Dr FERREIRA DA SILVA, LILIANE (BRAZILIAN PRESIDENCY); Dr MENEZES, CLAYTON (BRAZILIAN PRESIDENCY)

**Presenter:** Dr TAVEIRA, MARCIO (BRAZILIAN PRESIDENCY)

**Track Classification:** CC: National nuclear security regulations
Physical Security Proposing for Risk Reduction in Hypothetical Nuclear Fuel Fabrication Pilot Plant

Abstract - Physical security in nuclear fuel cycle facility means detection, prevention and response to threat, theft, sabotage, unauthorized access and illegal transfer involving radioactive and nuclear material. This paper proposes a physical security system designing concepts to reduce the risk associated with variant threats to nuclear fuel fabrication pilot plant. So, we will study the unauthorized removal and sabotage in a hypothetical nuclear fuel fabrication pilot plant considering deter, delay and response layers. Also, we will perform any required upgrading to the security system by investigating the nuclear fuel fabrication pilot plant layout and considering all physical security layers design to enhance the weakness for risk reduction through the fuel fabrication pilot plant inside and outside.

State

Egypt

Gender

Male

Primary authors:  Dr SALEM, Mohamed (Egyptian Atomic Energy Authority EAEA); Dr SALEH, Alaa (EAEA)

Presenter:  Dr SALEM, Mohamed (Egyptian Atomic Energy Authority EAEA)

Track Classification:  PP: Physical protection systems: evaluation and assessment
A Knowledge-based Insiders Trustworthiness Evaluation System (KITES)

The KITE System is one of the components in the Integrated & Intelligent Nuclear Security System (I2NS) that are currently under development in Malaysian Nuclear Agency, with the aims to enhance the capability for the insiders control and monitoring. KITES development involves the usage of mathematical modelling of the personnel trustworthiness to calculate the trust degree for each personnel in nuclear facilities. Apart from that, this system implements the semantic web technology to facilitates the required intelligent capabilities through inference and reasoning process during the trustworthiness evaluation. The development of this system requires a new ontology model for Personnel Trustworthiness Evaluation. For this purpose, a new ontology model have been developed to represents the information of personnel and its elements in the trustworthiness evaluation into a knowledge-based model. The newly developed ontology is then going through cycles of quality assessment process conducted by a number of subject matter experts following the multiple-criteria approach for ontology quality assessment as described by Burton-Jones et al.(2005). This paper aims at presenting the newly developed ontology and its quality assessment results.

State
Malaysia

Gender
Female

Primary authors:  IBRAHIM, Maizura; Dr AB HAMID, Amy Hamijah; Mrs HAMDAN, Siti Nur-bahyah; Mr HARIS, Mohd Fauzi; Mr ISMAIL, Saaidi; Mr MUHAMED ARIS, Sufian Norazam; Mr HASAN, Mohd Hasnor; Mr ASLAN, Mohd Dzul Aiman; Mrs ABD GHANI, Nur Fatini

Presenter:  IBRAHIM, Maizura

Track Classification:  PP: Insider threats
Efforts of the ROK to enhance nuclear security awareness

There have been many cases reported on security breached accident due to the lack of security awareness around the world. This awareness on security that was called security culture was especially important in the nuclear facility since its consequence was huge compared to other facility. The international community including the IAEA has been making efforts to enhance the awareness of nuclear security by discussing it as main agenda at nuclear security summit and publishing guidebook as one of the nuclear security series. The ROK, which has 24 nuclear power plants, has recognized the importance of nuclear security culture and has been conducting many activities to increase the awareness of nuclear security of those who works at nuclear facilities. The most effective ways to enhance the nuclear security culture is to provide education and training to the staff including managing members. The ROK had prepared legal base for mandatory training program on nuclear security in 2012. Every staff who works at nuclear facility should take training class for 2 hours to 8 hours depending on his/her job position mandatorily. A lot of hands-on activities were included in the program using the SETT (SEcurity research, Training and Test facility) located in the KINAC. In addition, the ROK had developed questionnaires to evaluate awareness of the nuclear security of the staff and has been conducting survey annually since 2009. The survey was made up of a series of questionnaires that were divided into four categories, beliefs and attitude, operating systems, leadership behaviors and staff behaviors. More than 800 persons who worked at nuclear facilities from over 10 different facilities had participated in the survey. Score of the awareness increases gradually. Analysis was performed on the results of survey to figure out what measures should be taken to enhance the awareness of nuclear security. Analysis results showed that the respondents satisfied the items like responsibility of mission, training & exercises, supervision & management, and awareness of information security. On the other hand, items such as job definition, motivation for those who work in the security area, importance of duties, and expertise were analyzed as those of which should be improved. The ROK has a plan to develop customized training program depending on the kinds of audience such as for senior management and safeguards officer. The survey will be also conducted continuously with more sophisticated questionnaires.

State

Republic of Korea

Gender

Male

Primary authors: Dr YOO, Hosik (Korea Institute of Nuclear Non-proliferation and Control); Dr JANG, Seong-soon (KINAC)

Presenter: Dr YOO, Hosik (Korea Institute of Nuclear Non-proliferation and Control)
**Track Classification:** CC: Nuclear security culture in practice with a focus on sustainability
National Nuclear Security Regime In The State Of Kuwait: Role Of The IAEA

The cooperation with the IAEA is guided in particular by the directions and priorities defined in Kuwait’s Integrated Nuclear Security Support Plan (INSSP), whose one of the key objectives is to "establish formal governmental organization and measures for managing the national nuclear security regime" and which focusses on addressing immediate and future national nuclear security needs and priorities. The INSSP has proved to be an effective mechanism supporting a holistic strategic and graded approach to strengthening the country’s nuclear security regime and plays a key role in channeling efforts and resources towards achieving in the shortest time possible a strong and sustainable nuclear security infrastructure. Its implementation makes an important contribution to the overall security in the country through strengthening institutional, human and technical capability in various aspects of nuclear security, including control and securing of radioactive sources, national response plan, illicit trafficking and border controls. The INSSP’s scope covers all required components from the legal and regulatory framework to prevention, detection and response to prevent any unauthorized acquisition, supply, possession, use, transfer or disposal of nuclear and other radioactive material. The cooperation in the field of Nuclear Security started in 2006 where the first INSERVE mission took place followed by many meetings that led to the establishment of the INSSP in 2009. The IAEA support is extremely vital in establishing the Nuclear Security Regime. In this context, special efforts are being deployed by relevant stakeholders to strengthen further the national system for the security of radioactive materials to secure their protection against any malicious acts. The present paper outlines the cooperation with the IAEA and the significant steps undertaken and activities carried out to this effect and stresses in terms of lessons learned the importance of stakeholders’ involvement to achieve this goal.

State

Kuwait

Gender

Male

Primary author: Dr ALAWADHI, NADER (KuWAIT INSTITUTE FOR SCIENTIFIC RESEARCH)

Presenter: Dr ALAWADHI, NADER (KuWAIT INSTITUTE FOR SCIENTIFIC RESEARCH)

Track Classification: CC: Use of IAEA and other international guidelines for building national nuclear security regimes
Lesson Learned from Security Culture at National Border Management Agencies: A Case study in Indonesia

Lesson Learned from Security Culture at National Border Management Agencies: A Case study in Indonesia

Mr. Werdi Putra Daeng Beta1, Mr. Rustama2

1Indonesia Nuclear Energy Regulatory Agency (BAPETEN), Assessment Centre for Regulatory System and Technology of Radiation Facilities and Radioactive Materials, Jl. Gajah Mada No. 8 Jakarta 10120, Indonesia
2National Nuclear Energy Agency (BATAN), PUSPIPTEK Serpong, Indonesia

E-mail of the corresponding author: putradaeng29@gmail.com

Indonesia Nuclear Energy Regulatory Agency (BAPETEN) is a national government regulatory institution for nuclear energy utilization in Indonesia. BAPETEN controls nuclear energy utilization via regulation, licensing and inspection.

To prevent, detect and respond to incidents involving the illicit trafficking of nuclear materials and other radioactive sources are important for Indonesia. As a maritime country, Indonesia operates 9 international airports and 20 international seaports. It is necessary to ensure that we can effectively reduce the risk of the smuggling of nuclear materials and radioactive sources in these international gateways. Several terrorist bombings, and certainly it is unthinkable if the terrorist have had the access to such dangerous materials, such as nuclear material are other risks that should be considered carefully.

More importantly, Indonesia is also a part of the global community in combating nuclear terrorism. Indonesia fully supports international cooperation to enhance peaceful and security in the world, including nuclear security. BAPETEN and other relevant institutions, both government and non government, have the responsibility for combating illicit trafficking and the illegal movements of radioactive materials. National/State border Management Agency is one element of nuclear security for maintaining security culture for security of the country.

Objectives: To describe security culture profile in the state border agency to get the awareness of the probability of nuclear and/or radioactive illicit trafficking. Also, to gain security culture index and the information of the obstacles and challenges in implementing security culture into security action.

Methods:
Methods used in this research were literature study, interview with stakeholders, conduct survey and fill up the questioners related to nuclear security culture aspects and the function of radiation portal monitor (RPM) for vehicle and pedestrian.

Results:
(1) Security culture profile will be shown in pie charts and analyze the strengths and opportunities for some developments in the future. From the experience of this research, we have lessons learned that:
   a. Legal framework is not fully understood clearly yet in more detailed regarding the RPM and in terms of export and imports.
   b. It is necessary to analyze the exact position of the RPM, so that detection of radioactive-containing goods is effective.
   c. There needs to be coordination between agencies at the leadership level to understand the importance of the nuclear security culture and the handling of nuclear security event.
d. It is necessary to socialize on how to work with radiation sources safely and securely in fostering national nuclear security culture, because sometimes the operators or users are less aware of the potential dangers.

(2) The Nuclear Security Culture (NSC) Index value as of December 14, 2016 was 3.16 in scale maximum of 4. If it is converted to decimal value will be 78.98 (seventy eight point ninety eight). So that the quality of NSC obtained for border control institutions is B which is categorised as good NSC quality.

Conclusions:
(1) The value of each element of nuclear security culture is not found to be of poor value (value of C). Some developments needed in area of nuclear security perception into security action/habits.
(2) The index value of nuclear security culture in stakeholders of border control institutions is 3.16 which is equivalent to the conversion value of 78.98 with quality of B.
(3) Awareness of the threat of nuclear security will improve awareness in work practice and would become a nuclear security culture, especially for Front Line Officers. It is recommended that NSC shall be measured in period of 3 (three) to 5 (five) years.

References

Keywords: security culture, state border agency, RPM, FLO

State
Indonesia

Gender
Male

Primary author: Mr DAENG BETA, Werdi Putra (Nuclear Energy Regulatory Agency (BAPE-TEN))
Co-author: Mr RUSTAMA, Rustama (National Nuclear Energy Agency (BATAN))
Presenter: Mr DAENG BETA, Werdi Putra (Nuclear Energy Regulatory Agency (BAPE-TEN))

Track Classification: CC: Nuclear security culture in practice with a focus on sustainability
INSSP contributes to strengthening the Sudan nuclear security regime

The overall objectives of an Integrated Nuclear Security Support Plan (INSSP) are to identify and consolidate the nuclear security needs of an individual State into an integrated document that includes the necessary nuclear security improvements, as well as to provide a customized framework for coordinating and implementing nuclear security activities conducted by the State, the IAEA and potential donors. The INSSP is designed to identify actions required to ensure that a State’s national nuclear security regime is effective and sustainable, based on IAEA nuclear security guidance.

The purpose of the paper is intended to provide information regarding all activities being undertaken, or planned to be undertaken, by Sudan which has the objective of enhancing nuclear security regime and Maximize Benefits from Integrated Nuclear Security Support Plans (INSSP) Implementation. Sudan has worked using the INSSP mechanism to improve the nuclear security regime in generally recognized as distinct functional areas in the field of nuclear security that aim to protect against nuclear terrorism: 1) Legal and Regulatory Framework; 2) Threat and Risk Assessment; 3) Physical Protection Regime; 4) Detection of Criminal and other unauthorized acts involving material out of regulatory control; 5) Response to nuclear security events; and 6) Sustaining a Sudan’s nuclear security regime. And how Sudanese Stakeholders coordination and collaboration to implementation INSSP.

State
Sudan

Gender
Male

Primary author: Mr MAHMOUD HAMID MOHAMMED ALI, Mogahed (sudanese nuclear& radiological regulatory authority)

Presenter: Mr MAHMOUD HAMID MOHAMMED ALI, Mogahed (sudanese nuclear& radiological regulatory authority)

Track Classification: CC: Identification of national needs through the development of an Integrated Nuclear Security Support Plan
Since late 2011, Kenya has seen an upsurge in violent terrorist attacks. According to Kenyan security experts, the bulk of the attacks were increasingly carried out by radicalized youths who were hired for the purpose. Kenya’s hope of improving its ranking on the global terrorism index (GTI) have been dealt a blow because of these attacks. According to the Global Terrorism Index by the Australian-based Institute for Economics and Peace, a report that measures the impact of terrorism, Kenya took a nosedive from the 22nd most exposed country in 2017 to the 19th most exposed in 2018. In 2016, terrorist attacks involving shootings, grenades, or other explosive devices resulted in 122 fatalities. Potential terrorist threats remain in Kenya, including within the Nairobi area, along the coast, and within the north eastern region of the country. Kenyan official buildings like government offices and law enforcement personnel or facilities have been targeted and therefore extra security precautions are needed. The Kenya Bureau of Standards (KEBS) in collaboration with International Atomic Energy Agency (IAEA) established a Secondary Standards Dosimetry Laboratory (SSDL) and Non Destructive Testing Laboratory (NDT). The SSDL is the custodian of the National measurement Standards in the field of ionizing radiation and provides calibrations of industrial and medical of end users of equipment used within the East Africa region. The NDT is responsible for inspection and testing of samples using Magnetic particle, ultrasonic testing, Die penetrant and Radiography methods. The facility receive more than 50 equipments and samples foe testing yearly. The paper discuss Kenya experience in designing physical protection System, security management and safety to comply with prescriptive regulations. The objective is to avoid malicious use of radioactive sources so that adverse consequences are minimised. The identification of key characteristic of the approach to regulating the security of radioactive sources are necessary. Adequate means of responders to have sufficient capabilities to prevent adversaries from completing their work are important.

Physical protection systems: evaluation and assessment;

State

Kenya

Gender

Male

Primary authors:  Mr COLLINS , Omondi (Head of Dosimetry, Kenya Bureau of Standards); Mr DAVID, Makan Ole (Kenya National Police Service)

Presenter:  Mr COLLINS , Omondi (Head of Dosimetry, Kenya Bureau of Standards)

Track Classification:  PP: Physical protection systems: evaluation and assessment
Small Modular Reactors and Advanced Reactor Security: Regulatory Perspectives on Integrating Physical and Cyber Security by Design to protect against malicious acts and evolving threats

How can future nuclear technologies and Small Modular Reactors (SMRs) deter and prevent organized crime groups, terrorists and malicious actors from attempting to steal or sabotage nuclear materials and facilities. This paper presents the benefits of integrating Security By Design (SeBD) in regulatory frameworks to allow more flexible and effective design of physical protection systems for new SMRs. Under its effort to modernise the Nuclear Security Regulations, the Canadian Nuclear Safety Commission (CNSC) regulatory approach plays a key role in recognising the importance of SeBD in moving toward a performance based approach with less prescriptive requirements. CNSC also recognises the need for a graded approach using a risk informed criteria for nuclear security. As part of SMR Vendor Design Review process, CNSC reviews SeBD and interfaces with safety (robustness), safeguards (Nuclear Material Accounting and Control), operation and sustainability. CNSC also recognize the need to share relevant nuclear sensitive information from the national Design Basis Threat (DBT) with SMR designers so they can consider credible and future threats in their design. Finally, the interfaces between nuclear security and system engineer specialists within the VDR process allows to look at both physical and cyber security systems in a more holistic approach. This allows the regulator to look at how SMR developers intends to optimize nuclear safety to mitigate against potential acts of sabotage.

SeBD offers opportunities to reduce costs for new nuclear facilities. However, it is not a “silver bullet”. SeBD needs to be integrated as part of an overall security strategy taking into consideration the security policies, the facility characteristics, the material used and the national threat/DBT. In addition, there are outstanding security challenges to address such as: remote facilities without effective and timely off-site response capabilities, the intent of building unmanned facilities, the increase cyber security risks with the over reliance on digital technologies, the use of lethal force by autonomous and remotely operated security systems or protecting floating SMRs. These SMR designs are for future use, but now is the time to address some of these ethical questions that may shape the reality of future generations.

State
Canada

Gender
Male

Primary author: Mr DUGUAY, Raphael (CNSC)

Presenter: Mr DUGUAY, Raphael (CNSC)

Track Classification: PP: Nuclear security of new nuclear technologies (e.g., small modular reactors)
Secure Digital Asset Techniques

Introduction:
Nuclear security is the prevention of, detection of, and response to, criminal or intentional unauthorized acts involving or directed at nuclear material, or other radioactive material, associated facilities, or associated activities. As the uses of computers grow, so also the target space that criminals will try to manipulate either as tools for attack or as objects of attack themselves. United States (US) National Institute for Standards and Technology (NIST) framework prescribe that one should ‘develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services’.

Sensitive Digital Assts (SDAs) are sensitive information assets that are computer-based systems and need computer security measures for their protection. SDAs provide support systems for nuclear safety, nuclear security, nuclear material accountancy and control functions, store and process sensitive information related to such functions.

SDA is one for which if compromised, exploited, or failed, could impact the functions of the nuclear facility. The compromise of their confidentiality, integrity or availability (CIA) could lead to:
1. Unacceptable radiological consequences,
2. Theft of nuclear material,
3. Loss of sensitive information, or
4. A degraded capacity to prevent, detect and respond to a nuclear security event.

Digital Assets all have one or more of the following characteristics;
• They are of (high) value to the organisation.
• They are not easily replaceable without cost, skill, time, resources or a combination of all as the case may be.
• The loss or compromise of their CIA threatens the Organization’s functionality and prestige.
• They form part of the organization’s corporate identity.
• Their data classification would normally be proprietary, legal, highly confidential or top secret.

You cannot protect the devices that you cannot see or know anything about. One of the most important requirements is that organisations identify their SDAs support systems that perform nuclear safety, nuclear security or nuclear material accountancy and control functions, or that store and process sensitive information related to such function. Clearly understand the organisation’s digital assets, including:
• Where the assets are physically located and their functions in the network.
• The network connectivity and information flow.
• The consequences of any combination of loss of CIA on these assets.

Securing the SDAs is an attempt to describe the protection of a very complex and expanding set of programmable electronic devices and their supporting architecture; ranging from main frame computers to programmable logic controllers (PLCs) with applications from nuclear power plant safety systems to physical security monitoring systems.

The objectives of the SDA Design Techniques are to,
1. Prevent – Stop unauthorized access to SDAs.
2. Detect – Tracking authorized user’s activities.
3. Response – Minimize, mitigate effects and aid timely recovery.

Designing security techniques requires a risk informed approach i.e. you know what the threat vectors, the likely causal agents are. The design techniques should meet certain requirements and possess certain characteristics. Efforts are made to ensure that the SDA techniques do not risk causing spurious or incorrect actions that could lead to plant trips, plant equipment damage, or worse, accident conditions.

Design Techniques:
Digital Assets are diverse and there is no one protection solution or design technique fits-all. However, there are certain design techniques that are invaluable in securing our SDAs, such as; Design Basis Threat (DBT), Ruggedized Devices, Graded Approach, Defense in Depth, SDA Hardening, Physical Protection, Detection, Delay and Monitoring Capability, Penetration Testing, Regulatory/Industrial Compliance and Incident response, to mention but a few.

**State**

Nigeria

**Gender**

Male

**Primary author:** Mr OCHEME, Innocent (Nigeria Atomic Energy Commission (NAEC))

**Presenter:** Mr OCHEME, Innocent (Nigeria Atomic Energy Commission (NAEC))

**Track Classification:** CC: Information and computer security considerations for nuclear security
Reconceptualising Nuclear Security as a Business Enabler: Opportunities and Challenges

Monday, 10 February 2020 16:30 (15 minutes)

Synopsis

This paper will outline the potential benefits of taking a business-orientated approach to nuclear security and the opportunities and challenges that may offer. It draws on experiences of UK industry and activities conducted under the UK Government’s Global Nuclear Security Programme (GNP) (formerly Global Threat Reduction Programme, GTRP), which has been designing and delivering international nuclear security education, training and support for more than 20 years. This work forms the basis of the Nuclear Security Culture Programme (NSCP), an industry-academic consortium dedicated to supporting operators, regulators, academics and government agencies around the world. Led by King’s College London since 2014, the NSCP is increasingly recognising the application of concepts from the field of business administration and strategic management to nuclear security. Reflecting this new approach, the NSCP’s workshops and other activities now often include business-orientated topics such as risk management, leadership and business assurance.

The recent Nuclear Security Summit process led to an unprecedented level of attention directed towards nuclear security and helped to consolidate an international consensus at the governmental level on the need to mitigate the risk of nuclear terrorism. However, since the summit process ended the political momentum driving reforms and innovations has slowed. Government commitment and leadership remain vital to maintain the international nuclear security framework, but it is increasingly evident that this also requires the active participation of industry actors and the private sector.

Nuclear and radiological source licensees around the world are demonstrating ever greater responsibility and commitment to securing nuclear and radioactive materials and sensitive information. This is a commendable achievement, and a development that is reframing the normative context for nuclear security practices and behaviours. However, there remains a major obstacle to further progress: namely, nuclear security still tends to be regarded as an economic burden for operators. Rather than nuclear security being viewed as an enabler in disseminating the peaceful uses of nuclear technology, this aspect of the nuclear enterprise is too often considered as a drain on the bottom line. This presents challenges for nuclear security personnel trying to negotiate security budgets with the management level or governing board within nuclear organisations. The relatively low level of recorded security incidents exacerbate such complacency, despite it being widely accepted that calculations on risk must also factor in likely consequences of a given scenario; in the case of a nuclear terrorism event, these would be catastrophic.

Drawing on interviews with nuclear security managers and other personnel, the paper will explore implementation challenges faced by stakeholders charged with responsibility for nuclear security. In so doing, it will propose new ways of conceptualising nuclear security as a business enabler. The paper will detail the approach of the NSCP to its international workshops and other activities, with a focus on how business and strategic management concepts can be articulated to reframe nuclear security as a core business function providing value. The development of these workshops is not a simple endeavour in view of the difference in civil nuclear programmes, the range of licensees and the diverse national contexts and regulatory systems*. Nevertheless, the NSCP has observed that a business-orientated approach has worldwide relevance. Indeed, the evolution in funding mechanisms for new nuclear power plants is likely to bring core business functions and their associated costs under greater scrutiny as part of the commissioning and construction process. Likewise, shareholders are increasingly concerned by broader issues such as reputational damage and corporate social responsibility.
In particular, the paper will focus on the topic of risk management which now features across the NSCP workshops and other training and educational activities. A risk management approach emphasises how risk identification, risk assessment, risk reduction planning and risk audits are key business assurance processes. These processes are designed to ensure that security arrangements are proportionate, appropriate and affordable. Nuclear operators are encouraged to create links between the component parts of the risk framework, namely: critical asset and vital area identification; threat assessment and risk appetite; and risk reduction treatment. In so doing, business value is placed on the reduction of security risks. There is also an emphasis on leadership, management and governance within this context, enabling risk management to be positively enforced across the organisation. The paper will present an innovative and interdisciplinary approach to the area of nuclear security, providing new insights on what might be termed a 'virtuous circle’** in aligning security best practice with business value.

*Participants at NSCP workshops include stakeholders from nuclear power plants, the regulator, government bodies and research, as well as those working with radiological sources at universities, healthcare, oil and gas companies, and other industries.

**For more on this concept, see Laura S. H. Holgate, ‘Virtuous Circles: Linking Business and Nuclear Security’, paper presented at the High-Level Panel on Nuclear Security, Norwegian Nobel Institute (8-10 June 2017).

State

United Kingdom

Gender

Female

Primary authors:  HOBBS, Christopher (King’s College London); TZINIERIS, Sarah (King’s College London, UK); SALISBURY, Daniel (CNS)

Presenter:  HOBBS, Christopher (King’s College London)

Session Classification:  Risks and benefits to nuclear security from innovations in other fields, including artificial intelligence and big data

Track Classification:  CC: Risks and benefits to nuclear security from innovations in other fields, including artificial intelligence and big data
Title: Human Resource Development in Nuclear Security Detection architecture– Case of Sudan

CONFERENCE: IAEA International Conference on Nuclear Security: Sustaining and Strengthening Efforts 2020
AUTHOR: BOKHARI AHMED MONEIR
Sudanese Nuclear and Radiological Regulatory Authority
Title: Human Resource Development in Nuclear Security Detection architecture– Case of Sudan

ABSTRACT
The risk of nuclear terrorism and illicit trafficking remains very real. There are large quantities of diverse radioactive material in existence, which are used in areas such as health, the environment, agriculture, and industry. The possibility of nuclear and other radioactive material may be used for terrorist acts cannot be ignored and would happen in the current global situation.

Identify that risk and measures to secure nuclear materials and radioactive source needed to make them the most effective tools for reducing this risk by a commitment to strengthen the protection and control of such material, and to establish capabilities for the detection system.

Therefore, according to IAEA, an effective nuclear security system requires the provision of capabilities to prevent, detect and respond to a criminal or unauthorized act with nuclear security implications, involving nuclear and other material. If the established capabilities are to remain effective, they should be developed systematically and sustained detection capability over the long term by the State.

In order to achieve to develop and sustainable nuclear security as general, it is important that a state makes a national commitment to adhere to international instruments, and national commitment results in implementing several elements for ensuring the protection of persons, property, society and the environment from harmful consequences of a nuclear security event.

All competent authorities and operators involved in nuclear security need to ensure they continue, education and training need in relation to nuclear security. That refers to the importance of education, research, training, and knowledge management initiatives among stakeholders, and policy preparing well and sustaining for personal involving in nuclear security.

Education and training play an essential role in ensuring that experts and competent authority are prepared and qualified to analyses national nuclear security detection architecture needs, to prevent and combat the threat of sabotage or the use of nuclear and radioactive material for malicious acts, and to prepare effective response measures to nuclear security events.

The technologies and procedures are developing very fast with the introduction of new equipment and techniques. At the same time they are, continuous loss of qualified personnel due to retirement, aging workforce carrier development, and administrative changes negatively affect the countries’ capabilities to carry out nuclear security responsibility at objective can be reached through comprehensive nuclear security regime, design it by good, and sustain approach.

An effective nuclear security regime is dependent on proper planning, training, awareness, operation, and maintenance, as well as on people who plan, operate and maintain nuclear security systems.

Sudan established with collaboration with IAEA the Nuclear Security Support Centres to provide nuclear security training, provision of technical advice and education to a state’s nuclear security ‘competent authorities’.

These initial efforts have laid the foundation for the expansion of nuclear security education, training, and technical support to various national organizations, including designers and users of physical protection systems, front-line officers, first responders and emergency response personnel, intelligence and law enforcement authorities, trainers, nuclear regulators, and policymakers in various areas of nuclear security.
In this paper, we outline the nuclear security regime in Sudan as well as international cooperation and the effort of Sudan to develop detection by education and training nuclear security competent authority and continues cooperation between stakeholders, Moreover, the gap where the state nuclear security detection architecture can be improved, the challenges to the implementation of an educational program and training on Nuclear Security and the importance of a possible partnership between the university, institution, the regulatory authority and another stakeholder with nuclear security responsibility to strengthen the nuclear security regimes.

**State**

Sudan

**Gender**

Male

**Primary author:** Mr MONEIR, Bokhari (Sudanese Nuclear and Radiological Regulatory Authority)

**Presenter:** Mr MONEIR, Bokhari (Sudanese Nuclear and Radiological Regulatory Authority)

**Track Classification:** CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
Public Outreach Campaign on collecting orphaned ionizing radiation sources as an effective element of building and maintaining nuclear security detection architecture for detecting radioactive materials in illicit circulation

To reduce the amount of abandoned radioactive sources, minimize terrorist threats, as well as threats to life and health of citizens, in Ukraine there was launched the project “Public Outreach and Information Campaign about the Amnesty of Ionizing Radiation Sources”.

Improper handling of ionizing radiation sources (hereinafter IRS) poses a serious danger to human life. The influence of such sources on the human body varies, depending on the intensity and type of radiation. Under certain circumstances, especially in case of misuse, even fatal consequences are possible. Any source outside the specialized enterprise poses a real threat to human life and health. Besides, it may cause unwanted interest. To avoid the threat, orphaned sources must be identified, localized and stored securely.

By today, orphaned IRS are detected in all regions of Ukraine. There were frequent cases when citizens owned IRS, which, for one reason or another, were not included in the state accounting system. However, people were afraid to hand them over, since there was a criminal liability for illegal possession and storage of such sources. Besides, people didn’t know where they can surrender IRS. Fear and lack of information prompted people to dump IRS to landfills that are not suited for storing IRS and radioactive waste (RW).

On 4 October 2016, the Verkhovna Rada of Ukraine adopted Law “On Amendments to Article 265 of the Criminal Code of Ukraine Concerning the Voluntary Handing Over of Radioactive Materials” (No. 1638-VIII, dated 4 October 2016), which exempts from criminal liability for the voluntary handing over of radioactive materials. This has significantly simplified the process of IRS handing over, their registration, inspection and inclusion into the state accounting system, transfer to controlled storage. However, even after this, there was no significant increase in the citizens’ actions to hand over ionizing radiation sources. The reason is the lack of a balanced, target audience-oriented public outreach campaign in the regions.

Thus, with the support of the US Department of Energy and the Oak Ridge National Laboratory, the project “Public Outreach and Information Campaign on the Amnesty Program of Orphaned Ionizing Radiation Sources” was launched. Dnipropetrovsk region is chosen taking into account its developed industry, which is widely using radioactive sources, and therefore there is a high probability of getting them into illegal circulation.

It is supposed to interest the population in the transfer of sources of ionizing radiation that are not in state registration to state specialized combines. Such sources, after appropriate registration and inspection, will be included in the state register of ionizing radiation sources or in the state register of radioactive waste. These measures will help detect radioactive materials that are in a trafficking and transfer them under regulatory control.

Along with this, preparations are being made for a wide range of informational and explanatory work on harm that may be caused by radioactive materials for human health and the environment if to deal with them in an improper manner. It will be made clear to the public that radioactive material trade is illegal and does not constitute significant value.

State Agency on Exclusion Zone Management has qualified personnel and equipment for the safe identification and extraction of sources, certified vehicles for their safe transportation, as well as places for safe storage of such sources. Ionizing radiation sources will be placed in special
repositories equipped with modern physical protection systems, which excludes the possibility of using IRS for criminal, including terrorist purposes.

The goal of the project is to raise public awareness of the danger of seizing and storing IRS and reduce the threat of nuclear terrorism.

The main tasks of the project:
- to develop a culture of behavior and a proactive stance on IRS handling of the public;
- to provide the information on decriminalization in the event of voluntary handing over of IRS (Article 265 of the Criminal Code of Ukraine) to the public;
- to secure the interaction of state authorities liable for responding to the findings of unaccounted IRS;
- to develop informational material for raising awareness of the population about IRS handling.

The project consists of 9 tasks that contain 23 subtasks. By today, information on the IRS of the Dnipropetrovsk region has been collected, departmental documents have been analyzed and there were created interdepartmental working groups. A detailed "Public Outreach and Information Campaign Plan" has been developed, identifying four target audiences, five public awareness criteria, criteria for assessing the success of the campaign, and means and types of communication.

The project in the Dnipropetrovsk region is a pilot one. In case of its successful result the same campaigns will be held in other regions of Ukraine.

State
- Ukraine

Gender
- Female

Primary author: Mrs ZINKEVYCH, Lyubov (State Agency of Ukraine on the Exclusion Zone Management)

Presenter: Mrs ZINKEVYCH, Lyubov (State Agency of Ukraine on the Exclusion Zone Management)

Track Classification: MORC: Preventing illicit trafficking of nuclear and radioactive material
Development of a Framework for Analyzing Impact of Emerging Technologies on Nuclear and Radiological Security

Rapid advancement in technological development has a profound effect on the world around us. In this context, the influences that these advances could have on the nuclear and radiological security are changing rapidly and dramatically. Nuclear operators and security stakeholders are already investing significant resources to address some of these new emerging threats and to also integrate new technological solutions into security systems. However, systematic understanding of this massive technology evolution is of vital importance to follow the trends and identify both potential vulnerabilities and opportunities to increase effectiveness, and prioritize investment areas.

This study was designed to enable decision makers to evaluate the potential impact of emerging technologies and the way those technologies are implemented on nuclear and radiological security, now and into the future. The main objective was to develop an understanding of: How might emerging technologies both create and address future risks to securing nuclear and radiological materials around the world?

To achieve the goals of the study a robust analysis framework was needed. Some of the requirements and constraints applied to this framework were:
- It should be capable of analyzing and comparing a large number (hundreds) of technologies and applications
- It should effectively define and address criteria relevant to nuclear and radiological security
- It should be scalable: be capable of adding and removing technologies as they emerge, or no longer of interest
- It should be flexible: be capable of focusing on more specific areas within a broad area of nuclear and radiological security

This paper describes the analysis framework that was developed by Sandia to perform a systematic analysis of a large number of emerging technologies and prioritizing them with regards to their impact on the field of nuclear and radiological security. Several examples of analysis and outcomes are also presented.
Track Classification: PP: Nuclear security of nuclear fuel cycle facilities: emerging technologies and associated challenges and complex threats
Increasing Log-Access Security System Based On Face Recognition

Monday, 10 February 2020 16:45 (15 minutes)

Today’s nuclear institutions are facing major security issues; consequently, they need several specially trained personnel to attain the desired security. This personnel may make human mistakes that might affect the level of security. The human face plays an important role in social interaction, identifying people. Using the human face as a key to security, face recognition technology has received considerable attention, very popular and it is used more widely because it does not require any form of physical contact between the users and the device. This system is composed of two parts: the hardware part and software part. The hardware part consists of a camera and a motorized microcontroller system, while the software part consists of face-detection and face-recognition algorithms software. A camera scans the person’s face and matches it to a database for verification. In this paper, we present an access control entering system to a must highly secured environments like nuclear/radiation environments. First, when a person enters to the zone in question, a real-time video stream is run by the camera and sent to the software to be analyzed and compared with an existing database of trusted people, and we propose an algorithm to detect and recognize the face of the person who wants to enter to the secured area and verify if he is allowed. The access door will be opened if the user is recognized and an alarm goes off if the user is not recognized.

State

Egypt

Gender

Male

Primary authors: Mr SOLYMAN, Ahmed (Radiation Engineering Department, National Center for Radiation Research and Technology, Atomic Energy Authority, Cairo, P.O. 11787, Egypt); Dr SAYED, Mahmoud (Radiation Engineering Department, National Center for Radiation Research and Technology (NCRRRT), Atomic Energy Authority, Nasr City, 11787 Cairo, Egypt)

Presenter: Mr SOLYMAN, Ahmed (Radiation Engineering Department, National Center for Radiation Research and Technology, Atomic Energy Authority, Cairo, P.O. 11787, Egypt)

Session Classification: Risks and benefits to nuclear security from innovations in other fields, including artificial intelligence and big data

Track Classification: CC: Risks and benefits to nuclear security from innovations in other fields, including artificial intelligence and big data
Abstract
In this work, a cyber security simulation testbed for Boiling Water Reactor is proposed. It is built up in the form of Client-Server. The Server being the reactor core and the Client being the control room. The Client performs continuous check on power level values of the reactor and runs machine-learning Intrusion Detection algorithm and. The performance of the proposed algorithm is evaluated on the KDD dataset after performing dimensionality reduction using Recursive Feature Elimination; which identifies the set of the KDD features that mostly affect the detection. The algorithm is compared with others yielding accuracy of 99.41%. The testbed simulates the dynamic behavior of the nuclear reactor by running a set of differential equations on the Server. The Server continuously communicates the reactor parameters to the Client to ascertain that there is no change in parameters due to disruption in communication. If discrepancy in parameters’ readings occurs, the reactor issues an alarm and displays the change graphically on screen. This initiates the operation of the machine learning algorithm to determine the type of abnormality; whether system fault or intrusion. The whole simulation is developed using LabView and Python.

State
Egypt

Gender
Female

Primary authors: Prof. KANDIL, Magy (Nuclear and Radiological Regulatory Authority, ENRRA, Cairo, Egypt); Dr SALAMA, may (Faculty of Engineering Banha university); Mr IBRAHIM, Ziad (Faculty Engineering, Banha University Cairo)

Presenter: Prof. KANDIL, Magy (Nuclear and Radiological Regulatory Authority, ENRRA, Cairo, Egypt)

Track Classification: CC: Information and computer security considerations for nuclear security
Quantifying Potential Target Attractiveness In Research Reactors And Associated Facilities

Monday, 10 February 2020 16:30 (15 minutes)

The present paper summarizes the work conducted by the authors working on the International Atomic Energy Agency (IAEA) Coordinated Research Project (CRP) on “Nuclear Security for Research Reactors and Associated Facilities (RRAFs)-J02006” and more specifically, Task 2 activities: “Comprehensive Measurement of Security Risk for Research Reactors and Associated Facilities (RRAF)”. Task 2 aims to determine a methodology to estimate/inform on the holistic security risk posed by the suite of radiological and nuclear targets at a RRAF. This methodology will allow comparison of risks posed by buildings within a site and sites within a country.

The work focused on analysing the “likelihood” dimension of risk and more specifically, identifying the attractiveness of the nuclear and radiological material as potential theft and sabotage targets. Attractiveness addresses the ease of access and simplicity of initiation of unacceptable consequences without considering the local threat environment or security system of the RRAF. Concerning the “consequences” element of risk, the focus of the work thus far has been on the health and economic impacts of an event.

The proposed approach assesses the attractiveness and potential consequences of the nuclear and radiological materials and then proceeds to aggregate on building level and for the entire facility. Since RRAFs typically contain multiple potential targets, we propose a methodological framework to identify which materials / buildings and facilities are at higher risk, by comparing dissimilar events and types of material.

The application of the proposed methodology is applied to the IAEA Hypothetical Atomic Research Institute – HARI and is presented.

State
Greece

Gender
Male

Primary authors: SFETSOS, ATHANASIOS (NCSR DEMOKRITOS); VARVAGIANNI, Melpomeni (NCSR "DEMOKRITOS", INRaSTES); TSOUROUNAKIS, IOANNIS (Institute of Nuclear and Radiological Sciences, Technology, Energy & Safety, N.C.S.R. "Demokritos"); CATSAROS, NICOLAS (National Centre for Scientific Research "Demokritos"); EK, David (Sandia National Laboratories); POTTER, Charles (Sandia National Laboratories); Mr SCHUSTER, William (NRC); Mr BULTZ, Garl (Oakridge National Laboratory); ADU, Simon; AGBENORKU, Obed (Nuclear Regulatory Authority); SHULL, Douglas (IAEA)

Presenter: SFETSOS, ATHANASIOS (NCSR DEMOKRITOS)

Session Classification: Research Reactor Security
Track Classification: PP: Research reactor security
Experiences from continuous improvement of nuclear security at CEADEN

The Centre of Technological Applications and Nuclear Development (CEADEN) is an organization of investigation, development and innovations destined to generate and diffuse knowledge; as well as, develop and market products and competitive services starting from the science and the nuclear technique, laser, optic and related. Inaugurated on October 28 of 1987 with the presence of the Mr. Hans Blix, then General Director of the International Organism of Atomic Energy (OIEA), it has been from their beginnings an installation leader of the application of the nuclear technologies in Cuba, also, regional reference for the nuclear equipment.

Between their principals radioactive installations highlight two facilities of investigation and several analytic techniques and of rehearsals not destructive. It provides besides a department of nuclear equipment. In order to materialize the objectives of investigation, development and technological innovation, it has an inventory of radioactive sources that include all the categories risk.

In the frame of the Plan composed of support at the physical nuclear security in Cuba (INSSP), the CEADEN has benefitted from the execution of a combined project with the OIEA in order to reinforce their system of physical protection. During the years 2014-2015 were installed systems of detection and observation for CCTV circuit, established a local station of alarms and installed other systems of protection reinforced with technique-engineering.

Among the challenges outlined is the continuous improvement of the security system and physical protection of radioactive materials implemented, so we are developing a training plan for the Department of Surveillance and Protection of the institution. This training has been divided into 3 stages

- Stage 1 Relationship of Radiological Protection concepts with Security
- Stage 2 Security application,
- Stage 3 Discussion of a case
- Stage 4 Table exercise.

Parallel to this challenge specialists of the instrumentation department are immersed in the design construction and implementation of the instrumentation of a monitoring system in real time (radiological surveillance) to interconnect it to the physical security system that was installed in the centre through the project together with the IAEA. This system will send the measurements to the Radiological Protection Officer of the entity and to the national alarm monitoring centre.

The commitment with the technological securities and physics come implemented since the high management until the base, for the one which the development of seminars of qualify and the permanent surveillance of the execution of the administrative procedures has played an important role.

The CEADEN provides has professional credited in the specialization of administration of the physical security of radioactive sources, in the completion of the basic module and Certified Nuclear Security Physician (CNSP) of the Academy of the World Institute of Nuclear Security (WINS).

The present work summarizes the introduction of good practices recommended internationally; as well as, the combined work of the entity user with the Competent Authority for the physical security, the Regulating Nuclear Center and the OIEA.

State

May 9, 2020
Gender
Female

Primary authors:  Mr PAREDES, Jorge Luis (National Centre for Nuclear Safety); Ms SOGUERO, Dania (Centre of Technological Applications and Nuclear Development (CEADEN) )
Co-author: M r TOLEDO, Rene (Centre of Technological Applications and Nuclear Development )
Presenter: Ms SOGUERO, Dania (Centre of Technological Applications and Nuclear Development (CEADEN) )

Track Classification: CC: Nuclear security culture in practice with a focus on sustainability
NUCLEAR SECURITY AS PART OF THE SECURITY OF MAJOR PUBLIC EVENTS

Background
State’s nuclear security regime provides institutional framework to protect persons, property, society and the environment from harmful consequences of a nuclear security event. Nuclear security to Major Public Events (MPEs) is a challenging task as it is relatively a new domain for the safety and security professionals. Securing MPEs against nuclear security threats requires effective utilization of available nuclear security systems and measures. Seamless interface between law enforcement agencies, public safety organizations, military and technical / scientific expertise is imperative to prevent, detect and respond to any criminal or unauthorized act involving MORC.

Pakistan’s Experience
Nuclear Emergency Management System (NEMS) is in place in Pakistan to deal with any nuclear security event and MPEs are covered under NEMS Implementation Plan. The model is based on IAEA and GICNT guidelines. Competent authorities and relevant organizations are nominated to support MPE with requisite capabilities.

During the last 10 years, Pakistan has gained significant experience to support MPEs i.e. visits of Chinese Premier (2013), Chinese President (2015) and Saudi Crown Prince (2019), Change of Army Command Ceremony (2013) and Pakistan Day Parade on 23 Mar 2019.

To support MPEs, necessary organizational structures, appropriate technical capabilities & resources and nuclear security plans have been developed and tested. Organizational structures and technical / scientific capabilities of Pakistan include:-

- **Radiation Portal Monitors** for scanning of vehicles and pedestrians at key entry points of venue.
- **Radiation Assistance Groups** equipped with Mobile Radiation Monitoring Lab, Personal Radiation Detectors (PRDs) and handheld detection / identification equipment.
- **Aerial Survey and Support Team** having fixed and rotary wing aircrafts with aerial radiation detection equipment.
- **Radiation Monitoring Teams** equipped with detection equipment to monitor transport routes / pathways as part of outer perimeter security.
- **Radiation Medical Assistance Teams** for rescue, triage and emergency medical response.
- **Nuclear and Radiological Emergency Support Centre** acts as nerve centre for planning and coordination to support MPE, besides capacity building of stakeholders.
- **Incident Command Centre** having necessary command, control and communication capabilities for situational awareness and response to any threat.
- **Public Announcement and Media Handling** having preplanned protocols and procedures.

Despite necessary organizational structures, technical capabilities and plans to support MPEs, challenges faced during operations have provided insight to further strengthen nuclear security systems and measures in the light of following:-

- **Threat and Risk Assessment**: Conducting realistic threat and risk assessment and timely sharing of information with all stakeholders is vital for mission success.
- **Transport Routes and Pathways**: Deployment of Radiation Monitoring Teams away from the venue on the main entry and exit points as part of outer perimeter security is an important defense in depth practice for deterrence.
• **Technical Capabilities and Resources.** Selection of different types of detection equipment to be employed during MPE (as per area, spectators, vehicles, routes and lanes) is critical to the success of event. The major challenge is speedy screening of large number of people and vehicles.

• **Multiple Organizations with Diverse Roles / Responsibilities** Planning and coordination among multiple organizations with different roles and responsibilities is a challenging task. It requires implementation of plans, SOPs, protocols, specialized training and seamless interface between response organizations.

• **Public Awareness and Media Handling.** A unified authority to provide credible information to reduce panic and anxiety among public in case of NSE.

**Conclusion.** Pakistan’s experience of providing nuclear security during various MPEs will be shared with participants of conference.

**References**


**State**

Pakistan

**Gender**

Male

**Primary author:** ZAFAR, Ajmal (Strategic Plans Division, Pakistan)

**Presenter:** ZAFAR, Ajmal (Strategic Plans Division, Pakistan)

**Track Classification:** MORC: Nuclear security as part of the security of major public events

The application of ionizing radiation sources in various sectors of the Nigerian economy pre-dates the establishment of the Nigerian Nuclear Regulatory Authority (NNRA) as the competent authority for nuclear safety and radiological protection regulation in Nigeria. The NNRA established by Act 19 of 1995 commenced operation in 2001. In early 2000, Nigeria recorded loss of control incidences involving radioactive material. Nigeria has hosted several IAEA missions such as the International Nuclear Security Advisory Service (INSServ) Mission, Radiation Safety and Security of Radioactive Sources, Infrastructure Appraisal (RaSSIA) Mission, etc. The overall objective of these missions was to assess Nigeria nuclear security needs and develop a plan of action for the improvement of nuclear security regime in the country. Based on the Missions recommendations, Nigeria saw the need to systematically document, assess and evaluate national nuclear security architecture. Precisely, one of the recommendations of the INSServ Mission was the development of Nigeria Integrated Nuclear Security Support Plan (INSSP). It contains a list of activities necessary for instituting effective nuclear security infrastructure in the country based on the gaps identified by the IAEA Missions to Nigeria. Nigeria in 2010 approved the first Integrated Nuclear Security Support Plan (INSSP). The INSSP is reviewed every three years in order to track the implementation progress as well as update the plan. It is unique as it takes into account nuclear security activities between the country and the IAEA and those undertaken through bilateral assistance. Through the INSSP Nigeria’s needs in terms of legislative assistance related to nuclear security, participation in international, regional and national training courses as well as education and most importantly building nuclear security capacity among national stakeholders are being addressed amongst others. The presentation, therefore is to highlight the importance of the INSSP in the Nigerian nuclear security architecture and the achievements recorded in the six functional areas of the Nigeria INSSP

State
Nigeria

Gender
Male

Primary author: Mr BELLO, Nasiru-Deen (Nigerian Nuclear Regulatory Authority)
Co-author: Mrs OFOEGBU, Ethel Ebere (Nigerian Nuclear Regulatory Authority, Abuja)
Presenters: Mr BELLO, Nasiru-Deen (Nigerian Nuclear Regulatory Authority); Mrs OFOEGBU, Ethel Ebere (Nigerian Nuclear Regulatory Authority, Abuja)

Track Classification: CC: Identification of national needs through the development of an
Integrated Nuclear Security Support Plan
Cybersecurity has become a cornerstone of nuclear security in modern NPPs, considering the place of digital equipment (including reactor control systems and reactor safety systems) in their design and operations. IEC SC45A decided in 2008 to develop an IEC standard on cybersecurity requirements (IEC 62645). The first edition was published 2014. As the development of digital I&C raises, a new edition of this standard was directly started after publishing in 2015, and additional standards, on coordination of safety and security (IEC 62859 started in 2012, published in 2016) and on security controls (IEC 63096 started in 2016), were set on track.

The paper presents in its first part the IEC and its Subcommittee 45A (Instrumentation, control and electrical power systems of nuclear facilities). It explains how the IEC cybersecurity standards fits to the IEC SC45A framework and to other IT security work like ISO/IEC 270xx series and IAEA work (NST045 and NST047).

In the second part, the three IEC SC45A standards focused on cybersecurity are presented in detail.

- The standard IEC 62645 gives the high level requirements and guidance, in particular for development and management of a cybersecurity program, for programmable digital I&C systems. It uses a graded approach and covers the entire security lifecycle on program level and system level, as well considers generic aspects of security controls. The revision principles for the second edition (started in 2016) are: (i) to adapt the structure and high-level principle with ISO/IEC 27001:2013 and ISO/IEC 27002:2013, (ii) to be consistent to relevant IEC 62443 controls and (iii) to rearrange the structure to consider the future second level documents on cybersecurity.

- The standard IEC 62859 is intended to help coordinating safety and cybersecurity issues. This standard is needed because safety requirements can have impact on cybersecurity measures and vice versa. The safety-oriented provisions are often well established, and the cybersecurity requirements and controls are often added. This can result in interaction and possible side-effects which must be considered on two levels: the architectural level and the individual system level. Additional organizational issues are shown. This standard is also on track to become an EN standard.

- The standard IEC 63096 focuses on security controls and provides a catalogue adapted for nuclear I&C contexts. The standard is currently under development and will be published in 2020. The chapters 5 through 18 exactly follow the structure of ISO/IEC 27002 clauses 5 through 18. IEC/ISO 27002 controls have been reconciled with the requirements of the nuclear I&C domain and, if deemed necessary, modified or extended. Additional information on the preservation (confidentiality, integrity and availability) and the control focus (prevention, detection) are given for each control. Their relevance for the security degrees from IEC 62645 and a baseline, and with respect to the different phases (development, engineering, operation), is considered.

As conclusion the IEC SC45A standards for cybersecurity brings a new and regularly updated set of guidance from IEC, in conjunction with IAEA and country specific standards, to the international community with regards to cybersecurity for nuclear facilities.
State
Germany

Gender
Male

Primary authors:  Mr WALTER, Thomas (PreussenElektra GmbH); PIETRE-CAMBACEDES, Ludovic (EDF); QUINN, Edward (Technology Resources); Mr BOCHTLER, Jürgen (Siemens AG)

Presenter:  Mr WALTER, Thomas (PreussenElektra GmbH)

Track Classification:  CC: Information and computer security considerations for nuclear security
A systemic approach to information and cyber security

Monday, 10 February 2020 12:00 (15 minutes)

Usually information is classified into different levels of sensitiveness which will dictate the measures for its protection. Information protection measures include barriers for access such as people clearances, cyber security, physical access controls, etc.

Also, Design Based Threat, or DBT, is a common principle for physical and cyber protection, which is based on threat assessments. Then, the security will be planned based on the risk assessment.

While we acknowledge the importance of the DBT, we argue that following this line of reasoning may limit our ability to grasp other vulnerabilities the system may have, because this follows the assumptions that:

a) The system will react according to the way we think it should, based on a predetermined fashion.

b) If each component of the system is reliable, then the system will be reliable.

However, nowadays technology evolves at fast pace, and the complexity of the systems is always increasing, with computer intensive machinery, allowing for interactions that had never been experienced before. Therefore, there are not enough data for statistical decision making. Also, very often we see accidents that could not be attributed to a single obvious cause, or root cause. The complexity of the interactions between the components of a system can lead to unwanted consequences due to unintended interactions, even if each individual component is working as it was supposed to.

Alternatively, systems theory assumes that accidents are caused by a number of systemic factors, and not by a single root-cause, generally a failure, that starts a chain of events leading to the accident.

Therefore, accidents are a problem of control of the interactions between the components of the system rather than a problem of finding root causes. The control of the interactions is represented by a hierarchical control structure, which is basically a representation of the system as a hierarchic structure where the higher levels control the interactions of the lower levels in order for the system to achieve the desired levels of safety and security.

A cyber security system can be approached as a socio-technical complex system, and in such humans are as part of the system as the computerized controls. In fact, human factors are present in every component of a socio-technical system, since all technological aspect is designed by humans. Therefore, of particular importance are the human factors, such as safety and security culture, and its effects on the interactions between all components.

Safety and security cultures are part of the organizational culture. The organizational culture permeates the entire system, as mentioned above, affecting decisions and, consequently, the interactions between the components.

Weak safety and security cultures will eventually contribute for the system to shift from a safe and secure state to hazardous states and, therefore, leading to losses or accidents.

This work analyzes the roles of organizational, safety and security cultures, as underlying factors that can lead to the deterioration of the hierarchical control structure, which is supposed to keep the interactions between the components of the system within desirable constraints.
Gender

Male

Primary authors:  Mr DE LEMOS, Francisco Luiz (CNEN _ National Nuclear Energy Commission);  Mr BIANCHI, Paulo Henrique (CNEN - National Nuclear Energy Commission)

Presenter:  Mr DE LEMOS, Francisco Luiz (CNEN _ National Nuclear Energy Commission)

Session Classification:  Identification, Classification, and Protection of Digital Assets in a Nuclear Security Regime

Track Classification:  CC: Information and computer security considerations for nuclear security
CYBER SECURITY APPROACH FOR NUCLEAR FACILITY; GHANA’S PERSPECTIVE.

Obed Agbenorku1, Simon Adu1, Kwame Appiah1
1. Nuclear Regulatory Authority

Abstract
The security of nuclear facilities is an important practice to prevent theft and sabotage of nuclear materials that could result in a radiological release. Traditionally, focus has been on physical threats to facilities such as armed militants gaining access to or damaging a facility. The newer trend for sabotage, theft and gaining access to nuclear facilities is cyber threat. Most operations in nuclear facilities have moved from the use of analog products to the digitization of operational functions and working processes increases in quality and efficiency. The digitalization of data and the extensive use of information management systems carried the world to a new era. The digitalization of infrastructure makes these systems vulnerable to cyber threats. The threat from cyber-attacks is now perceived as a problem of national and international security as cyber-attacks grow in number and the actors behind them are very knowledgeable in the field. Several nuclear facilities were designed without concern for cyber-attacks. This newer threat is presenting new challenges to facility operators as well as national authorities. Stuxnet has proven that even small electronic hardware components and their codes and drivers in the background are important for securing nuclear facilities. However, Stuxnet computer security incident demonstrated that nuclear facilities can be susceptible to cyber-attack. This and other events have significantly raised global concerns over potential vulnerabilities and the possibility of a cyber-attack or a joint cyber–physical attack that could impact nuclear security. The continues use of computers and other digital electronic equipment makes it likely target for cyber-attack that may affect physical protection systems at nuclear facilities, instrumentation, information processing and communications. Ghana’s plans on cyber security for its nuclear facilities and the up-coming establishment of nuclear power plant focuses on the following. Unauthorized access to information, Blockage of data transmission lines, Unauthorized intrusion into data communication systems or computers and Interception and change of information, software, hardware. The following concerns are also considered. Computer security which involves the protection of digital data and the defense of systems and networks against malicious acts, industrial control systems, access control systems, tracking and alarm systems, information systems pertaining to security and emergency response and adequate security measures during the introduction of hardware, software and the design stages. Cyber and physical security of facilities are put into categories or security zones to help protect each in a graded approach manner.

State
Ghana

Gender
Male
Primary author:  AGBENORKU, Obed (Nuclear Regulatory Authority)

Co-authors:  Mr ADU, Simon (Nuclear Regulatory Authority);  Mr APPIAH, kwame (nuclear regulatory authority)

Presenter:  AGBENORKU, Obed (Nuclear Regulatory Authority)

Track Classification:  CC: Information and computer security considerations for nuclear security
Building a National Nuclear Forensics Library and Provenance Capability in the UK

The International Atomic Energy Agency Incident and Trafficking database [1] records cases of unauthorised possession, theft, loss, transport and other unauthorised activities involving nuclear and other radioactive material. Intercepted materials can be analysed using nuclear forensic techniques to provide information to law enforcement and government. In addition, an advanced materials analysis capability, coupled with an understanding of nuclear fuel cycle signatures, can assist with determining a material’s history, for example, production processes, previous locations and intended use. A nuclear forensics library system that holds information on key signatures and material characteristics can be a powerful tool to support an assessment of the provenance of intercepted materials, particularly where there is a need to determine whether a material is consistent or inconsistent with a State’s holdings of nuclear and radioactive materials.

It is argued that a nuclear forensics library does not need to contain details of a State’s entire holdings (historic and current) and that adopting a concept of satellite libraries to hold a State’s information on nuclear and radioactive materials is a more pragmatic and proportionate approach. This concept relies on a State being able to identify exactly where specific information and expertise is located. It is proposed that a matrix that identifies the key expertise domains and information holdings within a State is aligned with another that identifies subject matter experts within each identified domain, thus facilitating rapid access to appropriate information and expertise.

Even the most extensive nuclear forensics library system and access to expertise may not be enough to facilitate a timely provenance assessment. How the experts work together to reach a mutually agreed assessment needs to be understood together with an understanding of how any assessment will be communicated to senior stakeholders, especially when statistical terms and confidence are being described. The UK has been developing a detailed but generic provenance process that clearly describes the way information will flow during an investigation and that promotes interaction and discussion amongst subject matter experts from disparate facilities.

This paper describes the UK’s recent work towards developing a nuclear forensics library, together with a detailed process for determining the provenance of nuclear and radioactive materials. This effort has been conducted in conjunction with developing expertise in identifying key signatures, developing data analysis tools and performing complex exercises to fully test the utility of the process.


State

United Kingdom

Gender

Male

Primary authors: AWBERY, Roy (AWE plc); EDWARDS, jeremy (National Nuclear Laboratory)
Presenters:  AWBERY, Roy (AWE plc); EDWARDS, Jeremy (National Nuclear Laboratory)

Track Classification:  MORC: Nuclear forensics
2018 French IPPAS mission – Experience and lessons learned

IPPAS missions play an important role to provide with an external review of a nuclear security regime and its implementation on a nuclear facility. France considers it as a very relevant tool developed by IAEA, whose legitimacy is internationally recognized, that can serve national authorities, according to their needs, to improve nuclear security globally. Internally as well, it can be a very good opportunity to raise the awareness of all the national stakeholders and to (re)create momentum.

France hosted its first IPPAS mission in 2011. During NSS 2016, President HOLLANDE stated that France would host a follow-up mission in 2018. The Ministry for an Ecological and Solidary Transition, competent authority in charge of the security of nuclear material, nuclear facilities and transports, hosted this new mission thanks to the support of its Department for nuclear security.

In 2011, the modules covered by the IPPAS mission were the following:
National review of nuclear security regime for nuclear material and nuclear facilities (module 1)
Nuclear facility review (module 2): visit of Gravelines NPP, one of the biggest in Western Europe, operated by EDF

The modules covered by the 2018 mission were the same as those covered in 2011. In addition, the IPPAS team reviewed module 5 dedicated to computer security. The facility chosen by France for the review of module 2 was the enrichment facility Georges Besse II, operated by ORANO. The report provided by the experts to the Ministry for an Ecological and Solidary Transition at the end of the mission concludes that "The nuclear security regime in France is robust and well-established, and incorporates the fundamental principles of the amended CPPNM". It also contains recommendations, suggestions and good practices applying both to the State and the operator ORANO.

The presentation aims at presenting the lessons learned from the 2018 IPPAS mission, from its preparation to the reception of the final report by the Ministry for an Ecological and Solidary Transition. The lessons learned cover different topics, including:
The selection of experts who came from different European countries,
The writing of the advanced information package sent to the experts before the mission,
The rehearsal of the mission,
The way different French stakeholders including ministries, authorities, technical support organization were involved in the preparation,
The type of information given to the experts to let them lead appropriately their mission (no classified information was necessary) and
The way the French authorities worked with the IPPAS team.

More broadly, the presentation deals with the French consideration on IPPAS missions and the different benefits its brings on a national and international scale. This presentation, among other things, aims to encourage countries, whose competent authorities in charge of the preparation have few human resources, to host them. It provides specific suggestions to adapt it to their needs and constraints.

State

France
Gender

Male

Primary author: LESAGE, Vincent (Ministry of Energy)

Presenter: LESAGE, Vincent (Ministry of Energy)

Track Classification: PP: International Physical Protection Advisory Service: good practices and lessons learned
Integrated Safety and Cyber Security Analysis for Building Sustainable Cyber Physical System at Nuclear Power Plants: A Systems Theory Approach

Nuclear power plants (NPP) install digital instrumentation and control (I&C) systems and physical protection systems (PPS) for its safe and precise operation using software-intensive systems and interconnected digital components respectively. The both of these software-intensive digital I&C systems and interconnected systems of PPS interface safety and security systems creating new cyber security threats that can lead to undesirable safety accidents in NPPs. Furthermore, the recent trend of attacks to nuclear installations may take place blended in nature that is cyber and physical attacks happening alongside. Consequently, these system designers encounter difficulties to incorporate these newly issued cyber security requirements in the additional design features of their safety systems. Therefore, integrated safety and cyber security analysis is indispensible part for building a sustainable cyber physical system in the NPPs. Despite the potential of integrating safety and cyber security analysis, NPPs addresses separately when they should not be. Drawing upon these limitations, this paper develops an integrated approach of safety and cyber security analysis at nuclear power plants based on systems theory. A system theory signifies the nature of a complex systems and represents a framework of investigation that later appropriated as Systems-Theoretic Processes Analysis (STPA). STPA is used as a unique safety analysis approach used on a large variety of systems today, including nuclear power plants (Young and Leveson, 2014). In the same way, extended STPA can provide a powerful foundation for cyber security analysis (Young and Leveson, 2014). In this study, we propose an integrated safety and cyber security analysis by combing STPA-Safety and STPA-Security methodology for building sustainable cyber physical system at NPPs. The proposed integrated STPA-SafeSec methodology provides a comprehensive analysis of safety and cyber security. The application of this novel STPA-SafeSec methodology is illustrated using a case study of a risk scenario in a nuclear facility.

NPPs critical digital assents of I&C systems are highly software-intensive which require strong assurance for safety and reliability. These digital I&C systems interface safety and security systems as it collect signals from sensors measuring plant parameters, integrates and evaluates sensor information, monitors plant performance, and generates signals to control plant devices using digital computers, communication system and network technologies. In the same way, a range of common software components, network management tools, operating systems of cameras, access control are gradually being integrated into the PPS infrastructures that support safety-critical system as well. The increasing use of these common components creates concerns that bugs might affect multiple systems across many different safety related components raising significant security concerns at NPPs. Both the systems are vulnerable to new cyber threats impacting on physical processes in a closed network though these systems of NPPs are isolated from real world internet. However, Stuxnet provides an example of blended attack covering cyber and physical processes that targets nuclear facilities though they are isolated from real world internet connection; where automated controller system thought the centrifuges( controlled process) were spinning at a slower speed than they actually were, and issued an increase speed command when the centrifuges were already spinning at maximum speed which led to equipment damage(concern officials probably wanted to prevent that loss; Stuxnet occurrence at Natanz Nuclear Facility, Iran in June 2010, October 2011, May 2012). Hence, both the digital I&C systems and PPS of NPPs pose a closed cyber physical systems which are critical for safe, enhance performance, convenient maintenance and precise operation. However, NPPs safety analysis methods do not consider these cyber physical
systems and also in the cyber security analysis, cyber security vulnerabilities does not often consider as critical, because their effects on the physical processes are not fully understood. Furthermore, literatures in this regards, reveal that several authors have studied the potential impact of security related threats on the safety of digital critical assets of nuclear facilities and highlight the importance of analyzing safety and security risks together (Kornecki and Zalewski, 2010). Therefore, concerns about approaches for NPPs that consider safety and cyber security analysis together are a primary need. Hence, this paper aims to analyze through considering the joint effect of cyber security and safety on NPPs that lead to major accidents. Consequently, this paper proposes a novel STPA-SafeSec methodology to providing a comprehensive analysis of safety and cyber security. The findings shed new light on straightforwardness of regulatory system that help to incorporating additional safety design features as well as to contributing mitigation strategy planning development for the emerging cyber threats in building sustainable cyber physical system at NPPs. Finally, this paper discusses the implications of the findings for research and practice.

State
Bangladesh

Gender

**Primary author:** Dr HOSSAIN, Md. Dulal (Bangladesh Atomic Energy Commission)

**Co-authors:** Dr ALAM, Md. Mahbub (Bangladesh Atomic Energy Commission); Mr ISLAM, Md. Shamimul (Bangladesh Atomic Energy Commission)

**Presenter:** Dr HOSSAIN, Md. Dulal (Bangladesh Atomic Energy Commission)

**Track Classification:** CC: Nuclear safety and security interfaces
Capacity Building of Regulatory Staff for Nuclear Security

Maintaining a sufficient number of highly skilled professionals, with appropriate academic qualifications and adequate experience, for regulatory supervision is of prime importance for regulatory bodies. This requires availability of a sustainable education and training program to build capacity of the regulatory staff through in-house training and retraining. Pakistan Nuclear Regulatory Authority (PNRA) adopted a proactive approach since its inception and started conducting in-house professional training courses and different methodology in the area of nuclear safety, radiation safety, radiation protection and Physical Protection.

PNRA also adopted a strategy to recruit staff that has basic and applied science knowledge by two way; induction of graduates from universities and graduates selected for fellowships for master degree in nuclear sciences programs. For an effective and systematic approach to the capacity building of the regulatory body, PNRA established a training center, National Institute of Safety and Security (NISAS) for the assessment of individual training plan and to conduct the formal training programme of its regulatory staff in light of regulatory body needs/requirements for nuclear safety and security. Based on the competence need assessment (CNA) and training needs assessment (TNA), PNRA trained its staff by different methods i.e. identification of competency gaps in legal, technical, regulatory practices and behavioral domains, establishment of a training centre for training of its man power including stakeholders, initiation of in-house training program for regulatory staff including hands on training sessions, commencement of a fellowship scheme for master degree program, attachment of staff at local/foreign institutes through IAEA for training and placement at various organizations for technical development with the assistance of International Atomic Energy Agency. The above strategies have been very beneficial in competence building of the PNRA staff to perform its regulatory activities indigenously not only for nuclear security and physical protection, but also for radiation protection and nuclear safety.

This paper summarizes the PNRA methodology to train its staff form the first step that is need identification to the final step that is evaluation of capacity building including policy making, implementation strategies (short and long term) for capacity building and determination of their competency needs. This also includes the measures taken for the competency development and subsequently enhancement of capacity building of its stakeholders including the support provided by the International Atomic Energy Agency (IAEA). The above methodology strategy is based on the competency model as given in IAEA Safety Report Series 79 “Managing Regulatory Body Competence” and using IAEA TECDOC 1757 “Systematic Approach to Regulatory Competence Needs Assessment (SARCoN).

State
Pakistan

Gender
Male

May 9, 2020
Primary author: Mr ASLAM, Muhammad Abid (Pakistan Nuclear Regulatory Authority)

Presenter: Mr ASLAM, Muhammad Abid (Pakistan Nuclear Regulatory Authority)

Track Classification: CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
INTERACTION BETWEEN NUCLEAR SAFETY SYSTEMS AND SECURITY SYSTEM USING LEU

Nuclear safety and nuclear security of Uranium Fuel Fabrication Facilities have the same ultimate goal to protect individuals, the public, and the environment from harmful effects of ionizing radiation. In uranium fuel fabrication facilities with low-enriched uranium 20% which uses in research reactors, large amounts of radioactive material are present in a dispersible form. This is particularly so in the early stages of the fuel fabrication process. In these facilities, the main hazards are potential criticality and releases of uranium hexafluoride (UF6) and U3O8, from which workers, public and the environment should be protected. Nuclear facilities are vulnerable to terrorist attacks or thefts of nuclear material, especially for fissile materials which can be used for nuclear weapons.

Nuclear Fuel in Research reactors typically use a form of uranium that is more highly enriched (20 %) than that used for power reactors, which may be a more attractive target for theft. For this reasons, safety systems in nuclear fuel fabrication facilities could be used to assist the security. Criticality Accident Alarm Systems (CAAS) are required in nuclear fuel fabrication facilities where an accidental criticality excursion could result from operational processes or insider sabotage. The systems could be integrated for safety and security protection by establishing procedural or automated alarm communications between safety and security disciplines for certain operational or event conditions to prevent the insider threat and mitigate the radiological consequence.

Scenario accident was demonstrated when the insider threat has motivation (political, financial, ideological, or personal) uses his experience and knowledge to do sabotage in nuclear fuel fabrication facilities during wet process intend to cause criticality accident.

State
Egypt

Gender
Male

Primary author: Dr ELSAYED, Hade (Egyptian Atomic Energy Authority)
Presenter: Dr ELSAYED, Hade (Egyptian Atomic Energy Authority)

Track Classification: CC: Nuclear safety and security interfaces
The Physical protection systems: evaluation and assessment

Monday, 10 February 2020 11:30 (15 minutes)

A physical protection system (PPS) integrates people, procedures, and equipment for the protection of assets or facilities against theft, sabotage, diversion, or other malevolent intruder attacks. The PPS functions are detection, delay and response, before the design of the PPS we must see what we must protect (facility categorization), what I must protect against (against which the PPS must be designed) and level of protection is adequate (facility categorization and data base threats). The design of the PPS can be implemented during the design of the facility or nuclear material. Before that we can trust the PPS we must make assessment and evaluation of the system to verify the effectiveness and see if the PPS verify the functions (detection, delay and response)

Before that we can trust if the PPS is adequate and effective, it must first be verified that it fulfills the essential functions: detection, delay and response.

This can be done with an assessment and depending on the response, an update is carried out. The assessment and overview must be done on different elements of the PPS and periodically and then evaluates the proposed design to determine how well it meets the objectives. In this work, we can see the assessment of different elements and if necessary the updates of equipment’s or procedures...

State
Morocco

Gender

Primary authors:  ABDELOUAHED CHETAINE, O (Center of Energy, Faculty of sciences university Mohammed V in Rabat Morocco); KABBACH, O. (Center of Energy, Faculty of sciences university Mohammed V in Rabat Morocco); BOUASSA, T. (Center of Energy, Faculty of sciences university Mohammed V in Rabat Morocco); SAIDI, A. (Center of Energy, Faculty of sciences university Mohammed V in Rabat Morocco); AMSIL, H (Centre nationale de l’énergie des sciences et techniques nucléaires, Morocco)

Presenter:  ABDELOUAHED CHETAINE, O (Center of Energy, Faculty of sciences university Mohammed V in Rabat Morocco)

Session Classification:  Physical protection systems: evaluation and assessment

Track Classification:  PP: Physical protection systems: evaluation and assessment
Education and training plays a pivotal role in the development and upgradation of overall security system. Specific training and education is necessary as new challenges evolve with time. After 9/11, the world scenario has completely changed in terms of security. With change of threat level, there is a need to improve, strengthen and revise existing education and training infrastructure. Nuclear Security education and training in Pakistan has been designed and delivered for awareness of employees involving in various activities of nuclear power programme, nuclear medical centers, agriculture centers and food industry etc. In this paper, the role of education and training in capacity building in Pakistan will be discussed.

Consequently, there is a dire need for highly qualified experts in nuclear security at the national level, since the responsibility for nuclear security rests solely with a State. At national level, Pakistan has established Centers of Excellence to serve as regional and international hubs for training and disseminating relevant know-how through three institutes: Pakistan Center of Excellence for Nuclear Security (PCENS), the National Institute of Safety and Security (NISAS), and the Pakistan Institute of Engineering and Applied Sciences (PIEAS). Pakistan Institute of Engineering and Applied Sciences (PIEAS) is ranked the No. 1 Engineering Institute of Pakistan by Higher Education Commission (HEC) of Pakistan. PIEAS offered MS (Nuclear Engineering) with specialization in nuclear security. PCENS is a state of the art training facility which offers extensive training on different areas of nuclear security and response. PCENS conducts various international training courses (ITCs) in collaboration with IAEA on nuclear security, inviting participation from foreigners from various countries along with local participants. It also houses a Physical Protection Exterior Lab (PPEL) established by PNRA which includes a range of state of the art physical protection technologies such as intrusion detection and access control equipment used for exterior applications as part of physical protection systems at nuclear facilities. NISAS conducts specialized courses to provide comprehensive training for effective regulatory operations.

Now a days, development of nuclear power programme and other nuclear applications is rapidly increasing worldwide. Due to this view, malicious acts related to nuclear and other radioactive material are prime issues of concern in the world. That is why the security of nuclear and other radioactive material is not limited to countries having developed nuclear programmes, but also equally important to countries having limited nuclear activities and to those countries which plan to expand their nuclear programme in the future. Experts and specialists in the field of nuclear security are needed to achieve the task of protection against any malicious act. Also, it is often seen that competent personnel leave an organization due to superannuation, change in career path and managerial changes. Ultimately, this has a negative impact on the State’s capabilities to carry out nuclear security activities in an efficient manner. Moreover, rapid evolution of technology can be attributed to introduction of sophisticated state-of-the art equipment and techniques.

Nuclear security personnel are involved in various assignments in Pakistan, including nuclear security detection, design of physical protection system, operation and maintenance of physical protection system, security contingency management etc. Different nuclear security assignments have different capacity building and training requirements. It is important to ascertain that nuclear security personnel can only perform their assignments effectively if they are given job-specific trainings. This also enhances their technical capabilities and create smooth interfaces with different management systems at a facility. This paper describes a program which is implemented in Pakistan for capacity building of personnel in the field of nuclear security focusing on job-specific trainings which is effective and can be used as a training module for nuclear security trainings.

**Key Words:** Capacity Building, Physical Protection, Nuclear Security
State

Pakistan

Gender

Male

**Primary author:** Mr AHMAD, ISHTIAQ (Pakistan Atomic Energy Commission (PAEC))

**Co-author:** Mr AHMAD, ALI (Pakistan Atomic Energy Commission (PAEC))

**Presenter:** Mr AHMAD, ISHTIAQ (Pakistan Atomic Energy Commission (PAEC))

**Track Classification:** CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
Radioactive sources are used, stored and handled for diverse nature of peaceful applications/purposes in Pakistan. Radioactive sources either sealed or unsealed are used in Nuclear Powers Plants, Nuclear Medical Centers, Food Irradiation, Industry, Agriculture and Research Institutes. Security measures for these sources are vital so that they may not become vulnerable target for adversaries. If these sources are not managed properly, loss, theft or mishandling of sources may lead to accidental exposure to workers and public.

This paper will highlight the sustainability of security measures for special form of radioactive sources i.e. Sealed Radioactive Sources (SRS) by ensuring compliance with regulatory requirements. The basis for these measures is National Regulations on Security of radioactive Sources – PAK/926 and IAEA guidance level documents i.e. Nuclear Security Series. These measures have been implemented through a comprehensively organized programme viz. Accountability & Control Programme for SRS. Key elements of Accountability & Control Programme include development of SRS database, physical inventory verifications, periodic inspections for compliance evaluation, assessment of measures for detection, delay, response, implementation of two persons rule and recommendations for improvements of security management measures. The main purpose of Accountability & Control Programme is to maintain knowledge of the radioactive sources, for the purpose of deterring and detecting any action that could lead to its unauthorized removal or misuse. The essence of this programme is to ensure the sustainability of these measures through regular inspections and verifications by corporate level of Pakistan Atomic Energy Commission (PAEC).

The compliance with regulatory requirements is the fundamental tool for accountability & control programme. This programme also oversee measures related to management responsibilities to ensure security, risk assessment, Categorization system for SRS, receipt, labeling, inventory management, storage, leak testing, key control, record keeping and retention and effectiveness of physical protection system. The implementation of accountability and control programme is carried through assigning responsibilities to respective personnel i.e. operators, carriers, shippers, institutes heads etc. which are continuously in contact with the corporate management. It is ensured that the background checks, for all personnel authorized to access SRS, are proportional to the security level of the radioactive source and are in accordance with the national regulations.

The SRS data is collected from all radiation facilities on the prescribed form "Accountability and Control of SRS Form" covering the necessary information regarding each source that includes source identification number, physical form, date of purchase, initial activity and category etc. On the basis of the information collected, a comprehensive data base is being maintained at corporate level. The physical verification of SRS is being conducted using the physical verification checklists which are based on the national regulations and IAEA guidelines. Risk of loss and theft of SRS is managed by using robust physical protection measures i.e. detection, delay, access control using the concept of defense in depth and graded approach. It is ensured that the security measures, for each category of radioactive sources, should be consistent to applicable security levels. The sustainability of required security measures is ensured through periodic inspections and verifications. It is ensured that the tracking of SRS from its import to final disposal/return to supplier is properly maintained and are under strict regulatory control. Security culture is being promoted and periodic trainings & awareness programs are conducted in order to guide the relevant personnel having responsibility for use, storage and handling of SRS.

**Key words:** Accountability & Control for SRS, Nuclear Security Series, Inventory, Security Management
State

Pakistan

Gender

Male

Primary author:  Mr IQBAL, JAVED (Pakistan Atomic Energy Commission (PAEC))
Co-author:  Mr LIAQUAT, MUHAMMAD RIZWAN (Pakistan Atomic Energy Commission (PAEC))
Presenter:  Mr IQBAL, JAVED (Pakistan Atomic Energy Commission (PAEC))

Track Classification:  PP: National accounting and control measures of radioactive materials
The First Universitas Gadjah Mada’s Nuclear Security Training for Police and Security Officer

The increasing of the global nuclear security issues encourages the need to improve the competence of human resources in the field of nuclear security in Indonesia, especially for security officers. The Republic of Indonesia as an archipelago country which has around 17,000 islands connected by the sea. This condition makes the complexity of the nuclear security surveillance. The Nuclear Engineering Program of Universitas Gadjah Mada (UGM) as a member of INSEN has a moral responsibility to improve Indonesian human resources capability in the field of nuclear security. According to this need, Nuclear Engineering Program has been conducted a three days training for members of police and UGM’s security officer to improve their capabilities in dealing with nuclear security issues.

Several nuclear security related materials, such as Introduction to Radiation, Introduction to Radiation Detection and Measurement, Principles and Cases of Nuclear Security in the World, Nuclear Emergency Procedure, Nuclear Safety Psychology, Introduction to Nuclear Installations and Radiation Facilities, Introduction of Physical Protection Systems and Transportation Security, were lectured by faculty members, chair of UGM’s security officer and staff of Nuclear Energy Regulatory Agency (BAPETEN). The materials were delivered by teaching, table top exercise, practical and discussion methods. Based on the before and after training questioners, we could conclude that the understanding of participants on nuclear security could be improved. This understanding arises due to the material fit to the need, varied delivery methods and the participant’s awareness. Therefore, this training will be carried out again with several improvements in accordance with the feedback from the participants.

State
Indonesia

Gender
Male

Primary author: PUTERO, Susetyo Hario (Universitas Gadjah Mada)

Co-authors: Dr WIJATNA, Agus Budhie (Universitas Gadjah Mada); Dr AGUNG, Alexander (Universitas Gadjah Mada); Dr WIDI HARTO, Andang (Universitas Gadjah Mada); Mrs MUHARINI, Anung (Universitas Gadjah Mada); Mrs WIJAYANTI, Ester (Universitas Gadjah Mada); Mrs FARIDAH, Faridah (Universitas Gadjah Mada); Mr FERDIANSJAH, Ferdiansjah (Universitas Gadjah Mada); Mr SANTOSA, Haryono Budi (Universitas Gadjah Mada); Dr KUSNANTO, Kusnanto (Universitas Gadjah Mada); Mr MONDJO, Mondjo (Universitas Gadjah Mada); Dr PRABANINGRUM, Nunung (Universitas Gadjah Mada); Dr SIHANA, Sihana (Universitas Gadjah Mada INDONESIA); Mrs ROSITA, Widya (Universitas Gadjah Mada); Dr IMARDJOKO, Yudi Utomo (Universitas Gadjah Mada)

Presenters: Dr SIHANA, Sihana (Universitas Gadjah Mada INDONESIA); PUTERO, Susetyo Hario (Universitas Gadjah Mada)
Track Classification: CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
SAFETY AND SECURITY INTERFACES DURING LIFETIME OF A NUCLEAR POWER PLANT – NATIONAL EXPERIENCE

Nuclear Safety is defined as “the achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation hazards” while Nuclear Security is defined as “the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities”. Nuclear safety and nuclear security have same fundamental goal i.e. to protect the public, the property and the environment from harmful effects of radiations. Nuclear safety is meant for protection of incidents/accidents resulting in radiological releases due to human error, component failure, natural disasters etc. while nuclear security aims to protect malevolent human actions/attacks resulting in radiological releases. Although safety and security have common goals but both have different approaches and culture. A synergic approach for safety and security, throughout the lifetime of a nuclear facility/nuclear power plant, will augment the effectiveness of the common goal associated with nuclear safety and nuclear security.

This paper is intended to highlight the National experiences towards safety and security interfaces during lifetime of a Nuclear Power Plant. The paper covers the following areas of National experiences towards safety and security interfaces during the lifetime of a nuclear power plant:

- Identification of areas where nuclear safety and security share similarities;
- Identification of areas where nuclear safety and security differ;
- Identification of safety concepts, criteria, and operational practices which enhances protection;
- Integration of safety and security measures such that implementation of one does not compromise the other;
- Awareness of safety and security synergy;

Nuclear safety and security share similarities in various areas including design, construction, operation and other associated activities. For example; the containment building at a nuclear power plant serves to prevent a significant release of radioactive material to the environment in the event of an accident, while simultaneously providing a robust structure that protects the reactor from a terrorist attack. One more example is design of physical protection upgrades of Karachi Nuclear Power Plant (KANUPP); under the umbrella of IAEA-Pakistan Nuclear Security Cooperation Program. The design was prepared jointly by safety and security teams of KANUPP. The design of physical protection upgrades of KANUPP enhances the security of KANUPP along with following safety provisions:

- Easy access for emergency services
- Emergency exits
- Emergency evacuation routs

The areas where nuclear safety and security differs includes information sharing. As an example, safety requires information sharing on free and for all basis while security emphasizes on need to know principle. Safety establishes wide outreach for communication channels while security emphasizes on secure network.
Nuclear installations are designed by applying the defence in depth principle for both safety and security. Certain design criteria imposed for safety purposes may serve to reinforce security. As an example, the single failure criterion applied to safety systems requires the nuclear installation to be designed with a sufficient level of redundancy and/or diversification to ensure that safety functions are maintained. Single failure criterion demands that safety be maintained even if one set of equipment in the system fails. This design feature is helpful for security purposes as well. The redundancy in safety design also serves as security layers against adversaries’ actions i.e. by application of this criterion, adversaries’ must compromise several safety layers in order to cause a radiological release. To improve synergy between safety and security, following actions are also implemented at nuclear power plants;

- Plant Operations Review Committee
- Work planning and control Committee
- Design control and configuration management
- Quality assurance and audit

Nuclear safety and security must not be pitted against each other and one should not have ascendancy over the other. It is very difficult to envisage merging safety and security into a single entity; they must however coexist and reinforce each other mutually.

**Keywords:** Nuclear Safety, Nuclear Security, Synergy, Theft, Sabotage, Karachi Nuclear Power Plant (KANUPP).

**State**

Pakistan

**Gender**

Male

**Primary author:** Mr ALI, SYED RAFAT (Pakistan Atomic Energy Commission (PAEC))

**Co-author:** Ms SABIR, NOOR UL AIN (Pakistan Atomic Energy Commission (PAEC))

**Presenter:** Mr ALI, SYED RAFAT (Pakistan Atomic Energy Commission (PAEC))

**Track Classification:** CC: Nuclear safety and security interfaces
Nuclear security governance in the Indo/Asia-Pacific: Building out from Southeast Asia?

This paper explores pathways toward building a robust framework for nuclear security governance in the Asia-Pacific, building out from the nuclear security cooperation framework and progress in Southeast Asia. It argues that the progress made in Southeast Asia on building nuclear security cooperation can be expanded to the broader Asia-Pacific region. It explores potential policy pathways and practical collaborative mechanisms to export ASEAN norms and frameworks on transboundary issues (e.g., security, environmental issues) to the Asia-Pacific region to advance and improve nuclear security governance. Southeast Asia could be regarded as the test-bed for regional cooperation on nuclear safety and security, with key capacity-building cooperation initiatives from the ASEAN Network of Regulatory Bodies on Atomic Energy (ASEANTOM) as well as collaboration with other Asia-Pacific states such as Japan, South Korea, and China, among others.

As the driving force for regional interactions, collaboration offers an avenue for regional states to tackle emerging nuclear security threats and challenges to the civilian applications of nuclear technology and peaceful use of nuclear/radioactive materials. The importance of regional cooperation on nuclear safety and security is accentuated in the 2018 EAS Leaders’ Statement on the Safe and Secure Use, Storage, and Transport of Nuclear and Other Radioactive Materials. In this regard, the paper offers recommendations as to how regional nuclear security cooperation in ASEAN, primarily facilitated by ASEANTOM, could contribute to norms and frameworks on civilian nuclear governance in the Asia-Pacific. It identifies and argues for the relevance of ASEAN-led mechanisms to deal with nuclear security in Southeast Asia and the broader Asia-Pacific region—starting with the development of nuclear security culture. It analyses prospects for and emerging challenges to enhancing regional nuclear governance, covering three key issues: (1) nuclear security capacity-building; (2) the role of nuclear security centres of excellence and knowledge centres; and (3) nuclear emergency preparedness and response.

The specific objectives of this research are the following:

i. To identify and examine nuclear governance issues, national approaches, best practices and regional cooperation on civilian nuclear energy and radiological security in the Asia-Pacific;
ii. To explore and assess how ASEANTOM’s nuclear and radiological security capacity-building initiatives can be expanded to the Asia-Pacific;
iii. To discuss and evaluate the effectiveness of nuclear security border exercises and best practices in Southeast Asia and wider Asia-Pacific region;
iv. To explore and study how ASEANTOM’s nuclear emergency and preparedness initiatives can be expanded to the Asia-Pacific; and
v. To provide recommendations on and map out an agenda for a regional collaborative network of nuclear security centres of excellence and knowledge centres in the Asia-Pacific region.

State

Singapore

Gender

Female
Primary authors: Dr CABALLERO-ANTHONY, Mely (Professor and Head of the Centre for Non-Traditional Security Studies, S. Rajaratnam School of International Studies); Mr TRAJANO, Julius Cesar (Research Fellow, Centre for Non-Traditional Security Studies, S. Rajaratnam School of International Studies)

Presenters: Dr CABALLERO-ANTHONY, Mely (Professor and Head of the Centre for Non-Traditional Security Studies, S. Rajaratnam School of International Studies); Mr TRAJANO, Julius Cesar (Research Fellow, Centre for Non-Traditional Security Studies, S. Rajaratnam School of International Studies)

Track Classification: CC: Advances in nuclear security research and development; international cooperation on nuclear security research
Initial characterization of neutron sources out of regulatory control at the scene of a nuclear security event

The German Federal Office for Radiation Protection (Bundesamt für Strahlenschutz, BfS) has gathered considerable experience over the last decade in the identification and characterization of nuclear and other radioactive materials at the scene of a nuclear security event. This experience has been gained through numerous exercises, alarm exercises, training situations and deployments. The technical capabilities and expertise of the BfS is used, on request, to support either the police or radiation protection authorities during the response to a nuclear security event. In particular, the BfS can support nuclear forensics as part of an overarching police investigation. The measurement team structure of the BfS has been presented previously [1].

This contribution will focus on the initial characterization of neutron sources out of regulatory control at the scene of a nuclear security event. The initial, non-destructive, measurement of the dose rate (both gamma and neutron) with handheld detectors is used to characterize the source and, for californium sources, is utilized to estimate the age (time since last chemical separation) of the source. This information could be important for the police investigation of a nuclear security event and will be measured in the event that the source number is not readable (for instance if the source is damaged or has been tampered with deliberately). The results of dose rate measurements with several handheld detectors on californium sources over a range of ages (time since last chemical separation) will be discussed and compared with calculated results deriving from a combination of Monte-Carlo simulations and decay calculations using WebKORIGIN [2].

The contribution will show how simple, non-destructive measurements made at the scene can support radiation protection and nuclear forensics. Further non-destructive measurements with high purity germanium detectors can be made at the scene in order to gain further information to support nuclear forensics of californium neutron sources, for instance the age (time since the last chemical separation) or the presence of a Eu-154 impurity [3]. Our measurement equipment for these tasks, together with a discussion of the advantages and disadvantages of the chosen range of detectors, will be presented in the interest of sharing best practice. In particular, the response of various neutron detectors will be compared and the use of high purity germanium detectors in neutron fields will be discussed.

The challenges of maintaining a deployment-ready capability for the identification and characterization of nuclear and other radioactive materials in the field will be summarized and shared in this contribution, in order to contribute to lessons learned and good practice.

References


State
Germany
Male

**Primary authors:** Dr KESTEN, Jürgen (Bundesamt für Strahlenschutz); Mr GREGOR, Joachim (Bundesamt für Strahlenschutz); Dr BARON, Martin (Bundesamt für Strahlenschutz); Dr KROEGER, Emily Alice (Federal Office for Radiation Protection)

**Presenter:** Dr BARON, Martin (Bundesamt für Strahlenschutz)

**Track Classification:** MORC: Nuclear forensics
Discrimination of Different Nuclear Material in the frame of Nuclear Forensics

Nuclear forensics developed over the last decades as a consequence of illicit nuclear material seized outside its fuel cycle. Candidate materials in the back end of the fuel cycle include spent fuel and Pu retrieved from the reprocessing of the fuel. An important challenging task in nuclear forensics is the identification of the origin of the material, which is characterized by the type of the reactor where it was charged, its charge composition and the final burnup attained by the spent fuel. The required characteristic signature in a fingerprinting approach for the origin determination of a seized nuclear material is its isotopic composition. Then, a comparison of the composition of the seized material with that of materials of known origin covering a range of commercial reactor and fuel types could yield the origin of the seized material. The required origin would be that of the material with which the seized one exhibits the most similar isotopic composition. The comparison can be performed through fingerprinting approaches based on multivariate statistics or 3D isotopic correlations.

This work is a simulation study presenting a 3D isotopic correlation fingerprinting approach, with the axis of the 3D space reflecting ratios of isotopes used as characteristic signatures. In the case of spent fuel as the seized material, these would be ratios of fission products 134Cs, 137Cs and 154Eu measurable by NDA (gamma-spectrometry). In the case of the Pu, as the seized material, retrieved from the reprocessing of the spent fuel, the required ratios would be between the characteristic signatures 239Pu, 240Pu and 241Pu and total Pu measurable by DA (Thermal Ionisation Mass-Spectrometry).

The work assesses the potential of the approach to discriminate the different materials of the known origin considered. This is an important issue since a good discrimination would enhance the correct determination of the origin of the seized material. Different thermal reactors (LWR, AGR, MAGNOX, CANDU, RBMK) charged with different U fuels have been simulated for the purpose of the work, providing the material of known origin. The work focuses on spent fuel of low burnup (<3 GWd/MTU).

The procedure is found to be dependent on the inclusion of 234U and 236U in the charge composition of the fuel and it shows a potential to discriminate the reactor and fuel assembly types considered. Furthermore, the approach is sensitive to the half-lives of the isotopic signatures.

State
Greece

Gender
Male

Primary author: Dr NIKOLAOU, GEORGIOS (DEMOKRITUS UNIVERSITY OF THRACE)
Presenter: Dr NIKOLAOU, GEORGIOS (DEMOKRITUS UNIVERSITY OF THRACE)
Track Classification: MORC: Nuclear forensics
Niger System of accounting for and control of nuclear material (SSAC)

Synopsis

The establishment and maintenance of a national system of accounting for and control of nuclear material are very important aspects of the safeguard agreement signed for the obligations of a State under the Treaty on the Non-Proliferation of Nuclear weapons (NPT) because it contributes to nuclear security around the world.

Niger has signed and ratified these legal instruments with the IAEA and has put in place a National System of Accounting and Control of Nuclear Materials (SSAC) in accordance with the requirements of these agreements in order to establish that there has been no diversion of nuclear material from peaceful uses to nuclear weapons or other nuclear explosive devices in the state.

The Nuclear materials present are those used as radiation sources by mining companies, health and oil research for purposes of test of good operation of devices and calibration.

The country is also a Producer of uranium by some companies, and several uranium mining licenses are valid in the country each year. In addition, a nuclear power program is being implemented.

Therefore, Niger:

- Provide information to the Agency pursuant to these agreement, annually and quarterly,
- Facilitate access by Agency
- Cooperate with the Agency

The Additional Protocol reinforce the system and give to the IAEA inspectors complementary access and additional information. Apart from, the physical inventory verification missions of nuclear material carried out by the inspectors of the Agency every year.

In order to take full advantage of peaceful nuclear applications in secure manner, Niger adopted the Nuclear Law on the Safety, Security and Peaceful Use of Atomic Energy in 2018, the aim of this law is to bring the national legislation framework up to standard. , and created in December 2016 a Nuclear Regulatory and Safety Authority (ARSN) to oversee these activities.

The authorities plan to continue working closely with the IAEA to strengthen the system by improving the training framework at the national, regional and international levels on nuclear material accountancy systems.

Also, the difficulties to control the whole territory, can favor the illicit traffic, the majority of the users are located at hundreds of kilometers of the capital, border control devices and the training of the control personnel are necessary;

In addition, the creation of a subregional network to promote the safeguards agreement and its additional protocol under the auspices of the IAEA can be a very effective solution for improving the system. To face these challenges, Niger needs to strengthen its human and material capacities.
Primary author: Mr DJIBO, ALI (ARSN Cab PM)
Presenter: Mr DJIBO, ALI (ARSN Cab PM)

Track Classification: PP: Nuclear material accounting and control
AN IAEA NUCLEAR FORENSICS COLLABORATING CENTRE IN HUNGARY: A PARTNER LABORATORY

The IAEA’s Collaborating Centre in Nuclear Forensics with the Hungarian Academy of Sciences Centre for Energy Research (MTA EK) in Budapest, Hungary provides the Agency’s Member States with a leading partner laboratory enabling coordinated research, provision of applied training, access to advisory expertise, and mentoring opportunities that have allowed the IAEA programme of nuclear forensics assistance to flourish during the past decade. The alignment of subject matter expertise with laboratory infrastructure for the response to a nuclear security event distinguishes this nuclear forensics partnership and promotes its availability within central Europe and beyond. The Centre for Energy Research is further positioned to provide specialized and effective solutions in nuclear forensics in its role as part of the IAEA Nuclear Security Support and Training Centre network. Because the IAEA, as only an assistance provider, does not conduct nuclear forensics examinations, the Centre for Energy Research provides access to a nuclear forensics laboratory that can implement IAEA guidance on the conduct of nuclear forensics examination with Member State partners as well as a hub for technical applications and innovation to advance nuclear forensics science as a preventive and response to a nuclear security event.

The Centre for Energy Research offers unique expertise and facilities as a Collaborating Centre in Nuclear Forensics. The Centre has a long-standing expertise in non-destructive analysis that is built around core competencies in high resolution gamma ray spectroscopy to include medium resolution (NaI) and high resolution (high purity germanium) detectors applied to measurements of uranium (e.g. 232U, 234U, 235U, 238U) and their decay daughters (e.g. 230Th, 226Ra, 214Bi), together with age dating of materials by gamma-spectrometry. Expertise for nuclear forensics destructive characterization using sector field inductively coupled plasma mass spectrometry allows for age dating and interrogation of trace elements (actinides, major elements, high field strength elements, rare earth elements) incorporated in nuclear and other radioactive materials that provide insight to manufacturing processes, and in turn, material origin and history. The Centre’s scanning electron microscope with its energy dispersive analyzer provides information on microchemistry and homogeneity at the scale of less than one micron in addition to information on textures and surfaces also bearing on provenance. Further instrumentation is also helping nuclear forensics examination like infrared spectroscopy, X-Ray diffraction or neutron tomography. The Centre’s Nuclear Forensics Laboratory is further outfitted with facilities to receive and document nuclear forensics samples. Other capabilities include a hardened and secure facility for storage of seized nuclear and other radioactive material confiscated by the Hungarian authorities. Important to the capability base is a mobile capability to support law enforcement authorities in the response to a nuclear security event to include radiological surveys, evidence collection, establishment of a chain-of-custody and transport of this evidence back to the fixed laboratory.

Since the Collaborating Centre in Nuclear Forensics was established with the Centre for Energy Research in August 2016, the IAEA has embarked on a close partnership in nuclear forensics focused on implementation. Hungary has now participated in 3 IAEA Coordinated Research Projects in nuclear forensics to include studies of gamma spectroscopy as well as the development of digital systems to host a national nuclear forensics library, convened IAEA research coordination meetings, successfully piloted the IAEA Practical Introduction to Nuclear Forensics training to optimize skills of analysts in non-destructive and destructive analysis, and also served to inaugural the IAEA Residential Assignment in nuclear forensics where experts drawn from candidates from around the world are placed in the Centre’s Nuclear Forensics Laboratory for a period of approximately 3 months and instructed in all facets of planning, laboratory analysis, interpretation and reporting as required by law enforcement. The Centre most recently was the set for a short IAEA video portrayal to increase awareness and understanding of a nuclear forensics examination: https://www.iaea.org/newscenter/multimedia/videos/tracing-radioactive-material-with-nuclear-forensics
Over the past ten years, the Centre for Energy Research has become a model for nuclear security development and sustainability both through its designation as an IAEA Nuclear Security Support and Training Centre as well as the first Collaborating Centre designated by the IAEA Division of Nuclear Security. Through its ability to implement IAEA guidance on nuclear forensics in the field as well as its laboratory as well as to provide a high confidence skills, knowledge and expertise platform available to the IAEA and its Member States, the Centre is well positioned for further substantive contributions to assist States in meeting their nuclear security responsibilities.

State

Hungary

Gender

Female

**Primary author:** Mrs KOVACS-SZELES, Eva (Hungarian Academy of Sciences Centre for Energy Research (MTA EK))

**Co-authors:** Mr KOVACS, Andras (Hungarian Academy of Sciences Centre for Energy Research (MTA EK)); Mr SMITH, David Kenneth (International Atomic Energy Agency); Mr DAVYDOV, Jerry (International Atomic Energy Agency)

**Presenter:** Mrs KOVACS-SZELES, Eva (Hungarian Academy of Sciences Centre for Energy Research (MTA EK))

**Track Classification:** MORC: Nuclear forensics
NUCLEAR FORENSICS CAPABILITIES IN UGANDA: NOW AND THE FUTURE

There is widespread use of nuclear and radiological materials (radioactive sources and nuclear material) and technologies in the various practices and applications in throughout the world. In Uganda, these materials are used in medicine, agriculture, industry, research and education etc. Uganda has declared interests in embarking on the development of nuclear energy resources and technology for the generation of electricity. This coupled with the high rates of growth in industry and medical care advancements imply a continued rise in the use of nuclear and radioactive materials in the region and thus will consequently increase the likelihood of occurrence of radiological or nuclear incidents if not properly managed.

The current security situation and recent events in Uganda, the East African region and the world further assert the existence of the nuclear terrorism threat. It is known in current times that there are terrorists out there that are interested in obtaining nuclear or radiological materials with the aim of fabricating an improvised nuclear devise or a radiological dispersal and/or exposure device for terrorism purposes.

Following a nuclear security event or a radiological or nuclear incident, the types of evidence that may be collected include the radiological or nuclear material itself, referred to as radiological evidence, and traditional types of evidence that may be contaminated with these materials, referred to as contaminated traditional evidence. Traditional uncontaminated evidence is in many cases present and must be handled such that contamination is prevented. Upon collection of evidence that includes nuclear or radioactive materials, it is very important to conduct a forensic analysis of the seized materials to obtain crucial information to enable a successful investigation. It is thus imperative for Uganda and all states in the establishment of response measures and systems for nuclear security events to take nuclear forensics into consideration as key component.

Uganda’s nuclear security regime is coordinated by the Atomic Energy Council with active participation of other key stakeholders like the national police, the intelligence service, the defence forces, users of radiation sources and more. There are some capabilities in terms of equipment and technical personnel in the regulatory body, some universities and the national police. However, there are at present minimal measures and arrangements for their coordination and optimization for the strengthening and consolidation of the state’s nuclear forensic capabilities. It is also of concern that there are no visible cross-border bilateral or multilateral cooperation mechanisms in nuclear forensics.

The paper will deeply assess the current situation as regards capabilities and arrangements for nuclear forensics in Uganda. It will describe the existing capabilities in the different institutions within the country identifying gaps and strengths. It will further generate recommendations for improvements in the national capabilities and establishment of arrangements for international collaboration and support in line with recommendations of the International Technical Working Group on Nuclear forensics (ITWG) and with lessons from international best practices.

State
Uganda

Gender
Male
Primary author:  Mr SSEGGANE, RICHARD (Atomic Energy Council - Uganda)
Presenter:  Mr SSEGGANE, RICHARD (Atomic Energy Council - Uganda)

Track Classification:  MORC: Nuclear forensics
The overarching objective of nuclear safety and nuclear security is to protect the public, property, society and environment from harmful effects of ionizing radiation. The focus of nuclear safety is to prevent nuclear accidents arising from the unintentional and inadvertent acts by implementing protection and mitigation measures at nuclear installation. Whereas, nuclear security aims to prevent accidents and other malicious acts involving nuclear and other radioactive material arising from intentional and criminal acts by taking deterrence, detection, delay, response and mitigation measures.

Safety is necessary, but not adequate alone to protect nuclear or other radioactive material from intentional and criminal acts. Similarly, security is essential, but not exclusively sufficient on its own to provide protection against radiological consequences arising from nuclear accident. Therefore, both nuclear safety and nuclear security is equally significant for the safe operation of a nuclear installation.

Pakistan Nuclear Regulatory Authority (PNRA), the national nuclear regulator, has adopted systematic approach and methodology to deal with the interfaces of nuclear safety and nuclear security. The systematic approach consists of the arrangements to ensure that both nuclear safety and nuclear security are mutually supportive and complement each other in minimizing the radiological risks. Legislative and regulatory framework has been established which defines roles and responsibilities for nuclear safety and security at national level. Regulations either developed or in developing phase address interface issues. Different aspects of security are covered in various safety Regulations such as "Regulations for Licensing of Nuclear Installations in Pakistan-PAK/909", "Regulations on Safety of Nuclear Power Plants Operation - PAK/913", etc. Specific requirement for assessing and managing interface between physical protection and safety is addressed in "Regulations on the Physical Protection of Nuclear Material(s) and Nuclear Installation(s)-PAK/925" which has been approved for promulgation.

Furthermore, the licensing process is also harmonized as PNRA issues single license/ authorization for both safety and security during lifetime stages of nuclear installations and such license/ authorization is issued only when the operator complies with both safety and security requirements. Joint inspections are conducted with a team comprising of both safety and security inspectors in order to identify and manage interface issues. A centralized emergency coordination and event reporting mechanism exists for both nuclear safety and nuclear security events. A rotation policy for PNRA employees has been adopted so that they learn about both safety and security of nuclear and radiation facilities by improving their skills and knowledge. Transparency with regard to safety related information, while confidentiality of security related information is ensured.

PNRA recognizes that both nuclear safety and security require their own expertise and methodology with understanding of each other’s disciplines and requirements. For this, trainings are arranged for the staff working in nuclear safety to get familiarization with nuclear security and vice versa. PNRA regulations address requirements for safety and security cultures. It is pertinent to mention that PNRA has also established methodology to assess safety and security culture at organizational level.

Nonetheless, PNRA recognizes that safety and security interface is easier said than to be done and there are many associated challenges at implementation level. These challenges include the overlapping issues of safety and security cultures; enforcement and criminalization related to nuclear safety and nuclear security violations; interface with cyber security; diversified knowledge and
experience requirements for personnel dealing in these two disciplines. Furthermore, at international level, few guidance documents are available to address technical areas of safety and security interface.

This paper will describe in detail the PNRA’s approach to deal with the interface of nuclear safety and nuclear security. It will also address challenges faced in the implementation of nuclear safety and security interface.

State
Pakistan

Gender
Male

Primary author: Mr AHMAD, Tufail (Government Official)
Co-author: Ms IFTAKHAR, Noreen (Government Official)
Presenter: Mr AHMAD, Tufail (Government Official)

Track Classification: CC: Nuclear safety and security interfaces
Development of Nuclear Security Regulations to Address International Obligations

The global nuclear security regime comprises of international instruments like CPPNM, United Nations resolutions and IAEA codes and standards. These instruments make States responsible for implementing nuclear security and development of domestic laws, regulations and institutions to govern nuclear security in the country and establishment of systems to prevent, detect, and respond to malicious acts involving nuclear or other radioactive materials & associated facilities. Adherence to international instruments in the field of physical protection and nuclear security for formulation of national legal and regulatory frameworks can contribute towards combating threat of nuclear terrorism and other malicious acts involving nuclear or other radioactive material and associated facilities or activities.

Pakistan is a responsible country and attaches highest importance towards global efforts to promote and strengthen nuclear safety and security internationally. Pakistan is party to all the important conventions related to nuclear safety and security that includes the Convention on the Physical Protection of Nuclear Material (CPPNM) and its 2005 Amendment, Convention on Nuclear Safety, Convention on Early Notification of a Nuclear Accident and Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency. In addition, Pakistan is also committed to implement United Nations Security Council resolutions 1373 (2001) and 1540 (2004) that address, among other things, the threat of nuclear terrorism and nuclear proliferation and is following Code of Conduct for the Safety and Security of Radioactive Sources along with its Supplementary Guidance on import and export of radioactive sources.

As a responsible nuclear state, Pakistan has incorporated the requirements of the above mentioned international instruments in the national legal and regulatory framework. A comprehensive regulatory framework has been established to perform the regulatory functions related to nuclear safety, nuclear security and physical protection. This regulatory system is part of a robust Nuclear Security Regime (NSR) established for prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities.

Pakistan Nuclear regulatory Authority (PNRA) is empowered to issue and enforce regulations to ensure physical protection of nuclear and radiation facilities in the country. In this regard, the national regulations on Physical Protection of Nuclear Material(s) and Nuclear Installations (PAK/925) are in final step of promulgation while the Regulations on Security of Radioactive Sources (PAK/926) have been promulgated in 2018.During the development of these regulations, State’s obligations under international instruments were also considered along with the national legislative requirements, best practices adopted by international community, current evaluation of the threat, operational experience feedback etc.

This paper will describe the approach followed by Pakistan for development of nuclear security regulations to address international obligations in the field of physical protection/nuclear security.
Gender

Male

Primary authors: ABBAS, MUHAMMAD (GOVERNMENT OFFICIAL); Mr RIZWAN, Muhammad (Government Official); SHAH, SYED MAJID HUSSAIN (official); Mrs NOREEN, Iftakhar (Govt. Official)

Presenter: ABBAS, MUHAMMAD (GOVERNMENT OFFICIAL)

Track Classification: CC: National nuclear security regulations
PNRA Technical Support Capabilities for Detection Technologies and Associated Challenges

The IAEA Code of Conduct on the Safety and Security of Radioactive Sources describes that in a State, the regulatory body should have the authority to monitor at all appropriate checkpoints for detecting the orphan sources during their course of operation and to ensure proper storage of such radioactive sources. PNRA has developed various regulations for the effective control of radioactive sources based on the concept of "Cradle to Grave". The national legislative and regulatory framework empowers PNRA for regulating and supervising all matters related to safety and security of radioactive materials.

The prevention of unauthorized use, storage and transport of radioactive materials requires the availability of a sustainable detection mechanism at national level. To ensure the sustainability and long term operation of detection mechanism, PNRA has established a Technical Support Unit (TSU) with complete spectrum of technical and scientific support capabilities. The capabilities include the preparation of equipment specifications as per end user requirements, acceptance and periodic testing to ensure the operation of equipment, protection and energy calibrations for optimization of equipment response. The TSU is also capable for identification of the fault in hardware and software of detection equipment and troubleshooting. At the national level, TSU is capable to provide technical assistance to the relevant stakeholders.

The radiation detection technologies available with TSU are Personal Radiation Detectors, Radionuclide Identification Devices, Contamination Monitors, Neutron Search Detectors, Radiation Survey Meter, High purity Germanium Detectors, analytical software’s for quantification and isotopic composition of radioactive materials. The procedures available with TSU describe the sequential process of use, analysis of radioactive materials, acceptance and periodic testing, calibration and maintenance of equipment. However, it is difficult for TSU to cover the full scope of repair, maintenance and calibration of software and hardware of equipment due to the challenges of compact design of the equipment.

The outcome of this paper will be to present the need of radiation detection equipment for the detection and interdiction of unauthorized movement of radioactive materials, technical and scientific capabilities of PNRA TSU for the testing, calibration, maintenance of radiation detection equipment and assistance to national stakeholders, challenges and recommendations for sustainable operations of radiation detection equipment. The challenges may include degradation of technologies with passage of time, requirements of refurbishment/up-gradation, maintenance cost and repair/replacement of compact design equipment. The recommendations may include technical specifications to promote modular designs, repair capabilities of end users and availability of spares for replacement of faulty component.

State
Pakistan

Gender
Male
**Primary author:**  ULLAH, ANAYAT (PAKISTAN NUCLEAR REGULATORY AUTHORITY)

**Co-authors:**  Mr RIZWAN, Muhammad (PNRA); Mr AHMAD, Sajjad (PNRA); Mr SALEEMI, Majid Ali (PNRA)

**Presenter:**  ULLAH, ANAYAT (PAKISTAN NUCLEAR REGULATORY AUTHORITY)

**Track Classification:**  MORC: Building and maintaining nuclear security detection architecture
Use of radiation detection instruments in laboratory practice for nuclear security education

In practice, it is important to know technical challenges of qualification and calibration of radiation detection instruments for the identification of radioactive and nuclear materials. In this context, the selection, procurement and use of suitable radiation measuring devices for the safe handling, storage and transportation of nuclear and radioactive materials has great importance in a facility. Because there are a variety of radiation detection and measuring equipment in the market. It is a very vital matter to know which of these devices to use for which purpose and to determine the measurement capabilities.

The purpose of this paper is to describe a perspective on the gained experience radiation detection instruments for the identification and characterization of nuclear and radioactive materials. This perspective may give some insights to overcome the challenges and benefit from the opportunities of the state-of the art of the technology related to radiation instruments.

For use of the available radiation detection instrument in nuclear security education, an academic nuclear security course for BSc students was conducted in three Academic Semester between 2017 and 2019 in Institute of Nuclear Sciences of Ankara University. In this course, practical exercises were carried out in the laboratory. One key parameter is the uranium enrichment of the uranium material for the characterization. For instance, for determination of the isotopic uranium abundance, gamma-ray spectrometry is a fast and cheaper one than other analytical tools due to its ease of use, portability, non-destructive nature in such applications in the nuclear security activities. This technique also allows analysts or first responders/front of lines on-site to measure and identify the radiation sources and materials. However, the uranium enrichment necessitates the use of specifically designed instrumentation and methods. To perform this in Nuclear Security Education activity in Ankara University, experimental setups were devised to use a gamma-ray spectrometer with Low resolution detector(NaI:Tl), intermediate resolution (LaBr3:Ce and CdZnTe) and high resolution (HPGe). The students were performed the regular experiments to determine 235U enrichment degree according to the Enrichment Meter Principle and Multigroup Analysis(MGA) methods. As a material, low enriched uranium( U3O8 in Certified EC-NRM171) certified reference materials (CRM) were used. In these experiments, uranium enrichment meter principle is based on use of 185.7 keV peak of 235U and MGA method uses 80-130 keV region of uranium spectrum. In each semester, about 20 students have already gained an experience on the calibration of a gamma-spectrometer with use of different types of detectors, obtained a perspective on the importance of knowledge of energy resolution, efficiency, experimental setup parameters such as geometrical factors, collimators and interleaved absorbers between sample and detector, and thus determining accurately 235U isotopic abundance in uranium samples.

In such a nuclear security education course, the encountered challenges, the gained experience on the use of radiation detection instruments, the pros and cons of gamma-ray spectrometry for nuclear security of nuclear and radioactive materials will be presented in detail.
Primary author: Prof. YÜCEL, HALUK (Ankara University, Institute of Nuclear Sciences)

Co-authors: Mr NARTTÜRK, RECEP BORA (Ankara University, Institute of Nuclear Sciences); Mr BALCI, SEFER (Ankara University, Institute of Nuclear Sciences); Ms SAATCI, SELIN (Ankara University, Institute of Nuclear Sciences); Ms KAPLAN, NESLİHAN CEREN (Ankara University, Institute of Nuclear Sciences); Ms BARUT, AYŞEN (Ankara University, Institute of Nuclear Sciences, Tandogan Campus, 06100 Ankara, Turkey)

Presenter: Prof. YÜCEL, HALUK (Ankara University, Institute of Nuclear Sciences)

Track Classification: MORC: Detection technology development and performance testing
RISK INFORMED APPROACH TO THE SECURITY OF RADIOACTIVE SOURCES IN USE AND IN STORAGE IN PAKISTAN

Radioactive Material (RM) is used in various areas like research, medicine, industry, agriculture and education for a wide range of applications in Pakistan. All necessary security measures are taken to prevent acquisition of radioactive sources in use and in storage against any malicious act causing any radiological hazard which may harm public, property, society and environment. By applying risk informed approach, Security of radioactive sources is ensured according to IAEA Recommendations “Nuclear Security Recommendations on Radioactive material and Associated Facilities (NSS-14)” and IAEA Nuclear Security Implementing Guide “Security of Radioactive Sources (NSS-11)”. In this paper, risk informed approach for secure management of radioactive sources will be discussed.

In the risk informed approach, we identify and assess threats and risks and develop, evaluate and implement alternatives to monitor and manage resulting actions for system effectiveness. A risk informed approach is necessary for prioritizing and designing nuclear security systems and measures. On the basis of threat and risk assessments, security of radioactive material is effectively and efficiently ensured.

Structured risk management approach is used at national level for reducing risks of any malicious acts at an acceptable level. At national level, all potential threats, related potential consequences and likelihood of malicious acts are assessed. In this perspective, a legislative and regulatory framework is in place for efficient and effective security of radioactive sources in use and in storage to address the threat. National regulator developed national regulations for security of radioactive sources which are in place.

In Pakistan, risk informed approach is applied on the basis of assessment of threat and risk, national regulator determines security requirements for radioactive sources. National regulator periodically evaluates the security level of radioactive sources according to present threat level. In this view, on the basis of national regulations and IAEA recommendations, physical protection systems and measures are developed and implemented for prevention of, detection of, and response to criminal or intentional unauthorized acts directed at radioactive sources. Security of radioactive sources is ensured throughout its complete life cycle. Any movement of radioactive sources through the country is done with prior approval of the national regulator. According to national regulations, all efforts are made to protect radioactive sources against assessed threat by ensuring provision of necessary resources to all stakeholders.

Threat is identified by identification of material, identification of adversaries, identification of targets and identification of consequences. After threat and risk assessment, we design physical protection systems and measures and implementation of these security measures. We are managing risk based nuclear security systems and measures by updated threat assessment, evaluation of the effectiveness of implemented nuclear security systems and measures. Potential systems and measures are identified which are deployed to reduce risk from any unauthorized act with implications of security systems. These systems include various access control systems, intrusion detection sensors and dedicated response force. These systems and measures are evaluated individually as well as in combination to identify risk reduction. Threat assessment is updated with new information about different adversary and their capabilities. Risk assessment is also updated with threat assessment is updated. In this view, we achieve effectiveness of risk informed approach for security of radioactive sources in use and in storage.

**Key Words:** Risk Assessment, Threat Assessment, Radioactive sources
State
Pakistan

Gender
Male

Primary author: Dr CHAUDHARY, MUHAMMAD TAHIR (Pakistan Atomic Energy Commission (PAEC))

Co-author: Mr LIAQUAT, MUHAMMAD RIZWAN (Pakistan Atomic Energy Commission (PAEC))

Presenter: Dr CHAUDHARY, MUHAMMAD TAHIR (Pakistan Atomic Energy Commission (PAEC))

Track Classification: PP: Risk-informed approach to the security of radioactive material in use and in storage
WINS Academy Programme: Sustaining Demonstrable Competency in Nuclear Security Management

The vision of the World Institute of Nuclear Security is that: “all nuclear and other radiological materials and facilities are effectively secured by demonstrably competent professionals applying best practice to achieve operational excellence”.

Protecting and security nuclear and other radioactive material and protecting material and facilities from sabotage requires nuclear security professionals that can clearly demonstrate their competency in delivering nuclear security. Professional certification is one of the most effective ways to demonstrate individual competence and to build, strengthen and sustain national capacity in nuclear security for the benefit of all.

A national nuclear security regime requires adequate financial, technical and human resources for each competent authority involved in its implementation as well as for the operating organisation that has primary responsibility for security. A sustainable national nuclear security regime requires human capacity for its continued effectiveness, especially at a time when nuclear energy and nuclear applications that support important societal objectives, health, industry, agriculture and culture may be subject to new and emerging threats based on advances in technology and increased capability of adversaries, including those motivated by violent extremist ideology.

Several States, private foundations, and the nuclear industry supported the development of the World Institute for Nuclear Security (WINS) Academy launched in 2014, as an initiative to provide practitioners involved in nuclear security with opportunities to earn certification in Nuclear Security Management through a programme of self-study and successful completion of proctored examinations. Underpinning the program is certification in accordance with external quality management standards. These standards provide an internationally recognized benchmark of quality; demonstrate credibility, competence and professionalism; and give potential employers and others in the industry an objective measurement of participants’ knowledge.

Recognising the importance of competence in nuclear security for both regulators and operators, internationally, WINS has obtained political and industry commitments to expand its Academy initiative, and these efforts were recognised at the 2016 Nuclear Security Summit in a Joint Statement on Certified Training for Nuclear Security Management led by Canada and the United Kingdom. This Joint Statement, signed by 35 States, was subsequently published as IAEA Information Circular 901 (INFCRIC/901), and commits signatory States to support the development of certification programmes for nuclear security, globally, through advocacy, peer review support, contributions or other means necessary. Other States, supported by industry and civil society, are being encouraged to join the INFCIRC and provide a tangible commitment in support of the WINS Academy and certified professional development for nuclear security.

A national nuclear security regime requires a diverse group of competent professionals that have a deep understanding of the principles and practices of nuclear security.

Central to a sustainable national nuclear security regime is a workforce of demonstrably competent nuclear security practitioners. At present the WINS Academy is the only available certification system in the world that allows practitioners to demonstrate their competence. It is in the interests of competence acquisition and maintenance that this model is further expanded, and all countries ensure that individuals with responsibility for nuclear security have access to certification programmes.

State
Other

**Gender**

Female

**Primary author:** Ms EVANS, Rhonda (WINS)

**Presenter:** Ms EVANS, Rhonda (WINS)

**Track Classification:** CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
WINS: Supporting the Sustainability of Nuclear Security Training and Support Centres

The World Institute of Nuclear Security’s (WINS) mission is to be the leader in knowledge exchange, professional development and certification for nuclear security management. One principal way in which it turns this mission into concrete action is to provide targeted support for the work of Nuclear Security Training and Support Centres (NSSCs), globally. Over the past decade, several States have established specialised national and regional centres for nuclear security training and technical support. The objective of these centres is to ensure that key stakeholders in a State’s nuclear security regime have sufficient human, financial and technical resources to carry out their nuclear security responsibilities. NSSCs support this goal by providing training and evaluation to ensure the effectiveness of their nuclear security systems over time. WINS programmes support NSSCs by contributing to the work of the International Atomic Energy Agency’s (IAEA) Nuclear Security Training and Support Centres (NSSC) Network. WINS has been a key contributor to the NSSC network since its foundation, serving as the original chair of Working Group B on Best Practices. Among other support, WINS led Working Group B to publish guidance on topics such as: identifying capacity and capability gaps for NSSCs, developing competency frameworks for nuclear security; developing metrics for NSSCs, implementing a national nuclear security strategy to sustain NSSCs, and implementing quality management systems. In 2017 experts from WINS supported the IAEA in its revision of IAEA TECDOC 1734 on Establishing and Operating a National Nuclear Security Support Centre (NSSC). The revised TECDOC considers the actual experience of NSSCs with a focus on providing guidance leading to the long-term sustainability of centres. This effort is aligned with the strategic objectives of WINS, which supports sustainable nuclear security practices and the development of internal capacity for nuclear security professional development. WINS has put these principles into practice through a cooperative effort, supported by the government of Canada, to work with the Mexican Secretariat of Energy (SENER) and provide technical expertise to its National Nuclear Research Institute (ININ) in the development of its national NSSC, called the Nuclear Security Training Centre (NSTC). Under this agreement, WINS supports ININ in achieving and maintaining external certification against quality management standards for the NSTC and its nuclear security training programme, producing learning materials in Spanish to complement existing WINS on-line training modules, running train-the-trainer courses and delivering nuclear security training events to selected participants in Mexico and in the Central American region. WINS plans to support additional NSSCs with similar projects that build internal capacity and are focused on long-term sustainability for developing nuclear security competencies in a State. For example, WINS has established an Advisory Group to bring together a group of likeminded NSSCs who have achieved, or are seeking to achieve, excellence in the delivery of learning services for nuclear security through the adoption of quality management standards. These initiatives are complementary to the work being undertaken by the IAEA and the NSSC network. Fundamentally, WINS believes in the importance of a wide variety of targeted programmes, implemented by a broad range of expert bodies, including non-governmental organisations like WINS, to assist all States in developing sustainable capacity for nuclear security.

State

Other
Gender

Male

Primary author:  Mr JOHNSON, Daniel (WINS)
Presenter:  Mr JOHNSON, Daniel (WINS)

Track Classification:  CC: Role of Nuclear Security Support Centers to support and sustain national nuclear security regimes
Strategic Approach Toward Nuclear Security Culture In Medical Institutions

The poster is to present the approach of strategic thinking in reference with mission, vision and the strategy of the non-nuclear facility such as hospital which is about to start shaping its culture of security.

In 2016 – 2018 the self-assessment of nuclear security culture in medical facility using radioactive sources has been done for the first time in Poland. The project was a great challenge for the research team from the very beginning. However, it was not very difficult to persuade the managers of the hospital to start with the project because they liked the idea of becoming the pioneers of nuclear security culture in Poland. The most challenging was to make the personnel of the hospital understand the importance of the nuclear security culture, the impact of the human factor on nuclear security in their small organization, and the significant difference between safety and security in general. There is no difference in meaning between safety and security in Polish language and the term security is mostly associated with as a physical protection, like in many other countries too. These first nuclear security culture self-assessments have become the mile stones for these small medical institutions. The nuclear security culture self-assessment project has initiated the nuclear security culture understanding among personnel and management. The hospital’s supervisors declared to continue, extend and develop the research to enhance the nuclear security culture. This encouraging management’s approach toward security culture made the researcher believe that it could be possible to implement the security into the organizational strategy. This is why, the next step would be to develop the strategy of medical institution with a culture of security.

State

Poland

Gender

Female

Primary author:  Ms WIŚNIEWSKA, Małgorzata (Poznan University of Technology)

Presenter:  Ms WIŚNIEWSKA, Małgorzata (Poznan University of Technology)

Track Classification:  CC: Nuclear security culture in practice with a focus on sustainability
Development of training for Member States on Maritime Search

This article describes the arrangements currently being worked on provision and promotion of training and enhancement of EPR capabilities of the Member States in the area of Maritime Search for illicit trafficking of nuclear and radioactive materials. The general Conference Resolution GC(57/RES/9 dated September 2013 – Article 70 requests the Secretariat to continue its efforts to develop, in close cooperation with Member States, guidance for States on how to respond to a maritime emergency involving radioactive material, and to continue discussion with interested Member States on how appropriate preparedness and response information can be made available to appropriate authorities, taking into account the requirements as regards nuclear security and safety.

Maritime transport remains the dominant mode for international trade both for bulk transport of commodities and containerized break-bulk cargo. The system of international maritime shipping handled approximately 230 million twenty-foot equivalent container units (TEU) in 2000, of which 31 million TEU (17 million actual container boxes) came through North American ports. Shipping containers account for 95% of U.S. import-export cargo tonnage. Under normal conditions, the system of international maritime transport depends on the ability to maintain a steady flow of container traffic through the world’s major ports. Efforts to achieve a secure system must not threaten the economic viability of the network and, by extension, the system of global trade. To be able to develop, acquire, and support the deployment of an enhanced national system to detect and report on attempts to import, possess, store, transport, develop, or use of unauthorized nuclear explosive devices, fissile materials, or radiological material happens to be an important goal for many Member States in order to deter, interdict and mitigate the use of nuclear or radiological materials for malevolent usage. In general, the Member States adopt a radiation detection strategy commensurate with the assessed threat of criminal or unauthorized acts or inadvertent movement of radioactive material. If a high level of assessed threat is present, the policy is to adopt a wide-ranging monitoring programme in which all border crossing points, maritime ports and airports are screened by the deployment of fixed installed RPM systems. Mobile equipment could be used as well for random search or target vehicles.

Development of a Maritime Capability for shipboard search is essential due to the threat from malevolent marine shipment of radiological material and in recognition of both operational and radiological challenges of shipboard search. Several aspects of a search aboard ship are unique. A ship may be stopped while underway at sea, on rivers, or in ports. Stopping a ship is a public domain event likely to attract media attention and, for this reason, a search must be successfully completed in a timely fashion. Furthermore, searches in confined or narrow spaces (e.g., between cargo containers) require the use of compact and highly portable search systems. Positive aspects of aboard-ship searches include immediate access to the shipping manifest and to knowledgeable, local guides for vessel exploration.

Measurements of gamma radiation by means of portable devices or easy-to-deploy fixed systems aboard ships reveal low backgrounds lacking most terrestrial components that are attenuated by the surrounding water. The overall gamma background rates are generally quite low, making the detectors more sensitive to man-made radiological material. Shipments containing TENORM materials should be taken into consideration occasionally. Both dose rate meters and gamma spectrometers are recommended for these measurements; the latter types with on-line evaluation capability are more advantageous. In contrast, the neutron background aboard ships relative to the
surrounding water has been observed to be elevated. A significant radiological challenge is the
Ship Effect, which is an excess of neutrons observed when approaching a ship isolated from land.
Elaboration of the Ship Effect will be made in the main article. The phenomenon of the neutron
background on or near a large ship is unique and attributed to cosmic-ray interactions in the ship’s
steel and cargo. This effect has become known as the Ship Effect. The Ship Effect is explained as
an excess of neutrons measured when approaching a ship constructed of conventional materials.
Teams approaching or boarding a ship with a neutron detector may interpret elevated neutron
count rates as a malevolent neutron source.

**State**

United States

**Gender**

Male

**Primary author:** MUKHOPADHYAY, Sanjoy (NS-IEC)

**Presenter:** MUKHOPADHYAY, Sanjoy (NS-IEC)

**Track Classification:** MORC: Building and maintaining nuclear security detection architec-
ture
Assessment of Security Measures and Systems for Radiological Facilities in Ghana

The security measures and systems for Radiological Facilities is considered to be an integral part of nuclear safety in Ghana. The changes made in ensuring and legislation of security following the establishment of new Nuclear Regulatory Authority. Regulation of radiation sources commenced in 1993 with the promulgation of the radiation protection instrument, LI 1559. Recently, the LI has been superseded by the nuclear regulatory authority Act 895 of 2015. The Act includes, among others, issues on safety and security of radiation sources, the regulation and management of activities and practices for peaceful uses of nuclear materials and radioactive sources, physical protection systems and the protection of persons and the environment. The Act established the independent nuclear regulatory authority in January 2016 and assigned the responsibility to regulate all radiation sources in the country. The basic concept and regulation in security and the effort made to strengthen the national regulatory programs of the nuclear materials and systems, as well as a brief survey of the radiological facilities in Ghana; experience in design, operation, inspection and licensing of the integrated security system for these radiological facilities; the upgrading of the security measures and systems at the different types of radiological facilities. The challenges of implementing security measures and systems are much more difficult now than in previous decades. The strategies used to protect the organization’s assets need to have a layered approach. It is harder for an adversary to reach their objective when multiple layers have to be bypassed to access a radiological facility along with the strategies that should be in place to implement the security at facilities using administrative, technical and physical controls. The main objective of the security systems and measures is to prevent the accomplishment of unauthorized obvious or obscured activities to nuclear facilities and nuclear materials. It is also to prevent radiological sabotage of facilities and theft of nuclear materials. Thus an effective system of security also plays an important role in preventing illicit trafficking of nuclear materials. The paper describes detail past and present of security measures and systems of nuclear facilities and materials in Ghana. This paper outlines the methods and measures used in security assessment of radiological facilities in Ghana. The facilities considered were the Gamma irradiation facility and the waste management centre both located at Ghana Atomic Energy Commission (GAEC). This will ensure effective compliance of requirements set by the regulatory Authority and international best practices.

State
Ghana

Gender
Male

Primary author: Dr OTOO, Francis (Radiation Protection Institute, Ghana Atomic Energy Commission)

Co-authors: Dr ADU, Simon (Ghana Nuclear Regulatory Authority); Prof. DARKO, Emmanuel
Ofori (Radiation Protection Institute, Ghana Atomic Energy Commission)

**Presenter:** Dr OTOO, Francis (Radiation Protection Institute, Ghana Atomic Energy Commission)

**Track Classification:** PP: Nuclear security vulnerability assessments
Cooperation Success Stories – Compliance to the new CSA N290.7 Canadian regulation

Emerging global threats are constantly evolving. The velocity of technology change within organizations is introducing different attack surfaces with new technologies and digital mobility. These along with increased regulation on cyber security is a challenge that many utilities and cyber security teams face for their security postures.

A new Cyber Security regulation, CSA N290.7 Cyber Security for Nuclear Power Plants and Small Reactor Facilities, was recently introduced and mandated by Canadian Nuclear Safety Commission (CNSC) for the nuclear power plants. Canadian nuclear utilities are starting to comply with this standard. The CSA N290.7 is a consensus-based standard developed with the participation of nuclear operators, the Canadian regulator, Canadian nuclear laboratories and key suppliers. The Standard addresses cyber security for the following computer systems and components: (a) systems important to nuclear safety; (b) nuclear security; (c) emergency preparedness; (d) Production reliability; (e) Safeguards; and (f) auxiliary assets or systems which, if compromised, exploited, or failed, could adversely impact item (a), (b), (c), (d) or (e).

The compliance timeline is different for each utility. Ontario Power Generator (OPG) is the largest energy generator in Ontario, where we are required to meet different regulatory requirements for different parts of power generation (i.e. Nuclear versus Renewable Generation cyber assets). OPG is the first utility that scheduled to meet compliance to the new CSA N290.7 regulation in November 2019. As the first Canadian utility, OPG has faced many challenges. In addition to complying with this new regulation, OPG has also addressed other emerging threats within cyber security.

A major issue has been addressing the supply chain third party risk. The information technology, and process control supply chain is complex, involves distributed system of interconnected networks, that is geographically dispersed and has many tiers of suppliers – from component manufacturers, to designers, integrators, and operators. This is not explicitly addressed in the current version of the Standard. OPG has worked closely with internal stakeholders and industry leaders to develop Cyber Security Provisions and incorporate these into contract Terms and Conditions. OPG has two levels of contract terms: baseline, and heightened requirements. The baseline requirements are applicable to all OPG’s purchasing agreements covering requirements for service providers that provide assets or services on regulatory assets. The Terms and Conditions have been included in all new contracts since 2017. OPG has been successful in this program rollout where we have continuously enhanced the program while sharing good practices and broader experience to enhance nuclear security through international working groups information exchange – as well as incorporating lessons learned from our main stakeholders.

State
Canada

Gender
Primary authors: Ms MAHDIAN, Parisa (Ontario Power Generation); Mr BENJAMIN, Mike (Ontario Power Generation)

Presenters: Ms MAHDIAN, Parisa (Ontario Power Generation); Mr BENJAMIN, Mike (Ontario Power Generation)

Track Classification: CC: National nuclear security regulations
IPPAS Missions – Three types of personal experience

IPPAS missions comprise a team of international experts who assess a State’s system of physical protection (nuclear security), compare it with international best practices and make recommendations for improvements. IPPAS missions were established in 1995 as a voluntary service to assist States in strengthening their national nuclear security regime. Initially IPPAS missions were mostly undertaken by States with relatively smaller or immature nuclear security regimes. However IPPAS missions were mainstreamed from 2010 after the first Nuclear Security Summit in Washington, which specifically encouraged all States to use and benefit from this service. There are now very few States with significant nuclear-related activities involving nuclear material that have never hosted an IPPAS mission.

IPPAS mission teams typically comprise 5-8 persons from IAEA member states having contemporary experience in a variety of nuclear security topics, including physical protection, transport security, response and computer security. Legal expertise is also required to address State legislation and regulations that implement nuclear security treaties. The availability of such experts and the leadership of the secretariat is vital to the continued running of IPPAS missions.

IPPAS missions are constructed around a series of modules addressing the State-level nuclear security regime, facility security, transport of nuclear material, security of radioactive sources, computer security and more recently the interface with nuclear accountancy and control.

The author of this paper has had the privilege of multiple experiences in being a member of an IPPAS mission team, being a team leader of IPPAS missions, and hosting IPPAS missions, including involvement in IPPAS follow-up missions. Each of these roles gives a different perspective on the effectiveness and sustainability of this successful service.

Without attribution to the countries involved (aside from Australia), or going into the details of individual IPPAS missions, this paper will outline the overall differing experiences made as a provider and receiver IPPAS missions. The paper will describe the key lessons learned from these experiences, establish some common conclusions and finally give suggestions for the evolution of the service in the years ahead. In particular, the paper will describe the commonalities and differences in being a host country contact, IPPAS team member and team leader.

The paper will also outline the vital role IPPAS missions play in the global nuclear security architecture.

State
Australia

Gender
Male

Primary author: BAYER, Stephan (Australian Safeguards and Non-Proliferation Office)

Presenter: BAYER, Stephan (Australian Safeguards and Non-Proliferation Office)
Track Classification: PP: International Physical Protection Advisory Service: good practices and lessons learned
CAPACITY DEVELOPMENT FOR RADIOLOGICAL CRIME SCENE MANAGEMENT IN UGANDA

There is widespread use of nuclear and radiological materials (radioactive sources and nuclear material) and technologies in the various practices and applications in throughout the world. In Uganda, the risky radioactive materials are widely used in medicine for diagnostic and therapeutic purposes, in road construction industry for density and moisture gauging, in industrial radiography, in well logging for oil exploration, and to a lesser extent in agriculture, for research and education. Further, the government of Uganda is considering introduction of nuclear energy in the energy mix and construction of an refinery, and an oil pipe line from the oil rich areas in western Uganda to Tanga port in Tanzania. These activities together with the already mentioned ones will increase the quantities and use of radioactive and nuclear material that are of radiological significance in case of an incident or accident.

Apart from the above peaceful uses, the current security situation and recent events in Uganda, the East African region and the world indicate that nuclear terrorism is probable as terrorist have in the past attempted to obtain nuclear or radiological materials for malicious purposes that might include fabricating of improvised nuclear devise or a radiological dispersal and/or exposure device and intentional exposure among other malicious acts.

It is thus imperative for Uganda and all states to establish a strong and well-coordinated mechanism for responding to nuclear security events and managing radiological crime scenes for purposes of preventing further intentional exposures to the public, contamination of the environment and crime scene management in case of evidence collection for prosecution purposes. The success in the investigation of a nuclear security event largely depends on the management of the crime scene and appropriate handling of nuclear forensic evidence that requires technical competences of all responders.

Response to nuclear security events mainly involves participation of a number of national agencies including Law enforcement, Emergency response organizations, Regulatory bodies and Technical support organizations. Such organizations exist in Uganda and have the relevant legal mandates for participation in the response activities. However, a harmonized and well-coordinated concept of operation for the response activities at both state and regional/local levels is yet to be established.

In relation to identifiable international best practices and IAEA recommendations from NSS22G, the paper will: (1) identify the national competent authorities and their roles for response to nuclear security events and radiological crime scene operations in the country; (2) provide recommendations on how to develop capabilities in relation to management of crime scenes,(3) Identify command, control and coordination arrangements and the roles and responsibilities of on-scene/operational personnel involved in radiological crime scene activities.

State
Uganda

Gender
Male
Primary author: Mr NIMBASHABIRA, Natharius
Presenter: Mr NIMBASHABIRA, Natharius

Track Classification: MORC: Coordinated response to nuclear security events
Enhancement of Nuclear Security Culture with Implementation of Nuclear Security Education at PIEAS

Nuclear Security education and training is very important for all personnel who are directly or indirectly involved with the nuclear industry. Pakistan Institute of Engineering and Applied Sciences (PIEAS) is the leading educational and training institute in Pakistan for master programs in various fields related to nuclear engineering and technology. Recognizing the importance of nuclear security education, PIEAS offers a sub-specialization in Nuclear Security in its MS Nuclear Engineering program to ensure its long terms policy of developing nuclear security expertise among nuclear scientists and engineers at post graduate level.

PIEAS started its nuclear security education program as subspecialty of its Master of Science (MS) in Nuclear Engineering Program in October 2009. Two courses, Nuclear Security and Physical Protection Systems have been offered regularly since then. These courses are offered to scientists and engineers who work either as operator or as regulator at various nuclear facilities. So far, 99 students have graduated with this specialty. It has been observed that nuclear security education at PIEAS has instilled security culture in their actions as second nature and is helping them in the development of nuclear security culture in their respective departments. The graduates who are working as operators have set a positive example for personnel by complying with nuclear security requirements, following nuclear security procedures, remaining vigilant, executing their work more diligently, and exhibiting high standards of personal and collective accountability by being a nuclear security culture role model. They have been able to promote an overall positive work environment by improving productivity, to reinforce safety-security interface by adhering to the better safety precautions, and to reduce the potential for an insider threat by decreasing the possibility that the facility personnel will perform, support, or ignore any malicious acts. Those who joined as regulators, have facilitated in updating the nuclear security regulations by upgrading the nuclear security and the physical protection requirements for nuclear materials and facilities. This has also made them capable of inspecting and evaluating (in collaboration with security personnel) the existing security systems, predicting their performance against changing threat scenarios, and stay ahead of evolving threats, capabilities and tactics by an intelligent adversary. An assessment process for nuclear security culture among the scientists and engineers, as per guidelines of IAEA, is currently in progress also.

This paper will present the experiences and lessons learnt related to enhancement of nuclear security culture by implementing nuclear security education for scientists and engineers working at various national nuclear facilities. The results of the nuclear security culture assessment survey will be presented. The significance and importance of interaction of PIEAS with other elements of Centre of Excellence (CoE), i.e., PCENS and NISAS, in improvement of nuclear security culture will be highlighted. The role of nuclear security educational labs, established recently at PIEAS in collaboration with IAEA and PNRA, in enhancement of nuclear security culture will also be discussed.

State

Pakistan
Gender

Male

Primary authors: Dr MAJEED, Tariq (PIEAS); Dr UL HAQ, Inam (PIEAS)

Presenter: Dr MAJEED, Tariq (PIEAS)

Track Classification: CC: Nuclear security culture in practice with a focus on sustainability
NMAC and Nuclear Security: Philosophy of Concept and Feasibility of Implementation

K.L. Ramakumar, Retiree, Department of Atomic Energy, Mumbai 400001, India
Email: Karanam.ramakumar@gmail.com

Nuclear security is one of the three important components of the triad namely Safety, Security and Safeguards. Soon after the IAEA came into existence, appropriate mechanisms in terms of documentation (agreements, conventions, Guides, both legally binding and otherwise) and modalities of implantation have been made available for safety and safeguards. Even though necessity of addressing nuclear security issues was recognised even earlier, it is only since the beginning of this century, this matter has attracted increased global attention.

Nuclear security is the responsibility of each individual State, but international cooperation is vital to support States in establishing and maintaining effective nuclear security regimes. Since 2006, the IAEA has issued Nuclear Security Series publications to help States to establish effective national nuclear security regimes. In 2015, the IAEA published Nuclear Security Series No. 25-G Implementation Guide: “Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities”. The main purpose of this publication is to focus on measures to prevent and mitigate the risk posed by insider threats.

An attempt has been made in this presentation to study

• Other parameters which could be potential candidates for assessing Nuclear Security particularly from the published literature of the IAEA
• Philosophy of using NMAC for assessing nuclear security
• Feasibility of applying NMAC as a tool for assessing nuclear security at different nuclear facilities and in different member states categories: no nuclear facilities, small quantities protocol members states, limited nuclear facilities, large nuclear facilities
• Role of MUF in assessing NMAC as a tool for assessing nuclear security
• Requirement of detection goals in terms of quantities (whether absolute quantities or relative quantities: the ideal situation for nuclear security assessment)
• Timeliness of detection
• The analytical methodology available for this purpose.

Based on the above study, it is inferred that application of NMAC even by a State with enough infrastructure and technical capability and despite having enough experience in meeting the safeguards obligations is quite challenging. Increasing merely number of material balance areas (MBA) may not result in minimising the challenges. The nature of fuel cycle activities, the total quantities of nuclear material and the type of nuclear facilities (item handling or bulk handling or material processing) determine the challenge of using NMAC as a tool addressing nuclear security. Typical examples are given to demonstrate this challenge.

The considerations of using NMAC as described above led to a broader conclusion that in most of the cases “Control” of nuclear material through administrative and technical means may be the first and critical line of approach followed by “accountancy” involving physical inventory taking of items containing nuclear material in the designated MBAs. Given the stringent requirements of accounting nuclear material with greater degree of accuracy needed for nuclear security and the achievable measurement uncertainties in the analytical methodology currently available, detailed accounting of nuclear material involving analytical measurements may not be feasible and in fact quite challenging. Thus, the philosophy of using NMAC system for nuclear security may be limited
to maintain and report accurate, timely, complete and reliable information on all activities and operations (including movements) involving nuclear material without involving detailed analytical measurements. The goal should be to maintain control over the nuclear material to ensure continuity of knowledge, and thereby to enhance the ability to deter and detect unauthorized removal of nuclear material. In the opinion of the author, it may be desirable to restrict the expansion of the acronym NMAC to "Nuclear Material Control" instead of "Nuclear Material Accountancy and Control".

State

India

Gender

Male

Primary author: Mr KARANAM, RAMAKUMAR LAKSHMINARAYANA (DEPARTMENT OF ATOMIC ENERGY)

Presenter: Mr KARANAM, RAMAKUMAR LAKSHMINARAYANA (DEPARTMENT OF ATOMIC ENERGY)

Track Classification: PP: Nuclear material accounting and control
Strengthening Nuclear Security through professional development and training: from best practice to successful implementation

Nuclear security itself is nothing new, with measures to prevent nuclear and other radioactive materials from becoming out of regulatory control and to detect their potential trafficking having existed since the start of the nuclear age. Additionally, the widespread use of radioactive materials for medical and industrial applications is therefore associated with the risk of theft of such materials with their potential use in criminal and terrorist acts. These increased threat concerns lead to clear consensus among security experts that nuclear terrorism is one of the greatest threats to global security and that strong preventative measures are needed to lock down nuclear materials around the world.

The success of the fight against illicit trafficking of nuclear and other radioactive materials necessitates the mobilization and interaction of different competent authorities such as police, customs, border guards, regulators, radiation protection and expert scientists. Each of these authorities has a role and responsibilities during nuclear security incidents that require a close interagency cooperation and interdisciplinary skills and an understanding of the technicalities involved with the detection, handling and analysis of nuclear or other radioactive materials. Thus, non-experts in the radiological field, such as front line officers, need to be familiarized with radiation detection, radiation hazards, and measuring and relaying technical information obtained from instruments for subsequent analysis by the scientific experts. This complexity and the need for optimized use of radiation measurement equipment obviously call for thorough training of the front line officer and the other competent authorities relative to their roles in the State’s national nuclear security plan.

Recent years have seen a surge of interest in nuclear security education and training courses driven by a growing international recognition of the importance of a strong nuclear security culture. Training is indeed considered as a systematic process through which a nuclear security organization’s human resources gain knowledge and develop skills by instruction and practical activities that result in improved States nuclear security capabilities. In that respect, national and international developments of training programmes shall ideally pattern the training for front line officers, their management, trainers and other experts in the field using adult learning methodologies and providing hands-on training using the actual threat materials and the detection equipment deployed. Consequently, several States and international organizations have launched initiatives in nuclear security training and education assistance as their contribution to enhancing the security of both nuclear and radiological material and know-how. Knowledge and expertise in this specific subject are, nevertheless, not enough to ensure that training is effective, thus focus is put on “train-the-trainers” (T3) sessions. This advanced course is to instruct selected participants on methodology to train pairs on how to best detect and respond to illicit trafficking of nuclear or other radioactive materials. The sessions are designed as strategic measure for cascading nuclear security related knowledge to the competent user groups in the Member States.

The international community has predominantly focused efforts at border and customs officials. Nevertheless, complementary efforts had to focus to assist law enforcement in thwarting the acquisition of nuclear and radiological materials by terrorists, by similarly increasing their capacity and capability to secure all materials and prevent a potentially catastrophic event from happening. The combination of individual and cross training all nuclear security involved stake holders of a State play a critical role in maintaining effective national-level nuclear detection architecture. With the view to keeping abreast of Member State’s needs in this particular area as their programme gain maturity, one can mention the support of the European Commission to international training activities with the help of its European Nuclear Security Training Centre (EUSECTRA) operated by the Joint Research Centre support. The concept of EUSECTRA has been highly in-
The European Commission through numerous support programmes from different General Directorates (namely DG TAXUD for Customs community, DG HOME for law enforcement community and DG DEVCO for EU foreign support) sustains building of multidisciplinary and cross agency capacity through training and exercises to prevent and respond to the terrorist and other criminal offences involving nuclear or other radioactive material.

Training for front line officers and proficient experts aims to be done in the most realistic way possible. Training centres use generally different small radioactive sources or simulated sources to inject radiation detection spectra into the radiation detector and thus produce “realistic” observables. Few training centres such as the EUSECTRA seeks to provide a “train as you fight” approach training by providing realistic scenarios with real special nuclear material. The training program offers then a unique opportunity for trainees to see and experience actual materials and commodities, as EUSECTRA is one of the few places in the world where a wide range of samples of plutonium and uranium of different isotopic compositions can be used for training in detection, categorization and characterization.

There is a clear consensus among training experts that Instructional systematic design (ISD) approach to curriculum development is critical to collaboration efforts, the efficacy of the resulting training and its portability across organizations and training centers. This approach has several advantages, it

• Provides framework for subject matter experts to contribute to the technical content of the material
• Helps ensure that stakeholder roles and responsibilities are appropriately incorporated into curriculum
• Promotes the development of progressive techniques, such as “flipped classroom” approach that enhances student engagement.
• Extends the impact when curriculum is implemented in regional centers such as EU Centres of Excellence and IAEA Nuclear Security Support Centres

The provided training courses shall aim to transfer practical knowledge and skills immediately applicable to participants’ professional responsibilities to combat illicit trafficking; stimulate and encourage inter-institutional communication and collaboration to combat illicit trafficking at the operational level; provide a standardized course format and materials that national partners can easily replicate after receiving initial training and assistance. Significant efforts may be granted to deliver an extensive range of equipment and apparatus to cover anticipated national or international customers commonly deployed and operated gears. Cross-over agency trainings and field exercises shall then support enhancement of efficient networking and capacity building.

This global approach in providing training and expertise dissemination is then expected to better meet the transfer and the dissemination of knowledge necessary to spread worldwide rigorous nuclear Security Culture and its successful implementation.

**State**

Other

**Gender**

Male

**Primary authors:** GALY, Jean (European Commission / Joint Research Centre); BAGI, János (In-
International Co... / Report of Contributions

Strengthening Nuclear Security th...

stitute for Transuranium Elements, Joint Research Centre, European Commission); KREVICA, Indra (EC JRC); MAYER, Klaus (European Commission - Joint Research Centre, Institute for Transuranium Elements); WALLENIUS, Maria (European Commission, Joint Research Centre, Institute for Transuranium Elements); KNOTT, Alexander (European Commission / Joint Research Centre); REGER, Gaston (European Commission /Joint Research Centre)

Presenter: GALY, Jean (European Commission / Joint Research Centre)

Track Classification: CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
Physical Protection Considerations during Decommissioning of Destroyed Nuclear Facilities and Sites in Iraq

Abstract:
The six major stages in the lifetime of a nuclear facility and of the associated licensing process are siting, design, construction, commissioning, operation, and decommissioning. The decommissioning stage includes activities that will ultimately lead to the removal of nuclear and other radioactive materials from the nuclear facility.

There are a number of destroyed sites within former Iraqi nuclear program which have been used for nuclear activities and which contain potentially significant amounts of radioactive material. Many of these sites suffered substantial physical damage during the 1981’s airstrike and 1991 Gulf War’s airstrikes and several have been subject to looting of materials and equipment as a consequence of the challenging security situation in the country after 2003’s Gulf War. All of these sites have high degree of contamination and require decommissioning and remediation in order to ensure nuclear safety and security. Many of these sites are located at Al-Tuwaitha Nuclear Research Site.

Al-Tuwaitha Nuclear Research Site (20 km to the south of Baghdad) was established in the 1960’s and grew to include three research reactors and facilities for nuclear fuel fabrication, radiochemistry, uranium enrichment, radioactive waste treatment, and biological research.

The strategic plan to decommission all nuclear facilities and sites in Iraq consists of three phases, which are (2008-2010) phase, (2011-2015) phase and (2016-2025) phase.

During a decommissioning phase of nuclear facilities, simply the physical protection and security measures should be maintained until removing of all nuclear and other radioactive materials. The level of physical protection and security measures will be down based on decommissioning steps, and other facilities such as radioactive waste storage facilities might be needed and should be considered with regards to physical protection as well.

The current paper discusses the considerations of physical protection and technical measures for decommissioned destroyed nuclear facilities and those nuclear facilities being decommissioned and generated radioactive waste at Al-Tuwaitha nuclear site to protect them against malicious acts and to enhance safety and security measures.

State
Iraq

Gender
Male

Primary author: Mr AL-HAMADANI, HAIDER (Iraqi Ministry of Science and Technology/ Radiation and Nuclear Safety Directorate/ Nuclear Security Division/ Al-Tuwaitha Nuclear Site)

Presenter: Mr AL-HAMADANI, HAIDER (Iraqi Ministry of Science and Technology/ Radiation and
Nuclear Safety Directorate/ Nuclear Security Division/ Al-Tuwaitha Nuclear Site)

**Track Classification:** PP: Nuclear security of decommissioned facilities and the facilities being decommissioned
Analysis of Nuclear Material Accounting and Control Technology in Spent Fuel Reprocessing Plant

After 60 years of development, China’s nuclear fuel cycle front section, including uranium exploration, mining, metallurgy, purification, uranium conversion, uranium enrichment, fuel manufacturing, has formed industrial capacity; however, the nuclear fuel cycle back section has not yet formed industrial capacity, we lack commercial-scale power reactor spent fuel reprocessing plants, and have not formed MOX fuel element production capacity, and there is still a gap with the nuclear power.

During the 13th Five-Year Plan period, China will strengthen the research of spent fuel reprocessing technology and build a 200-ton/year demonstration plant for spent fuel reprocessing. Meanwhile, China is planning to build an 800 ton/year commercial reprocessing plant with France.

Nuclear material accounting and control is an important part of operation and technological process control for spent fuel reprocessing plant. Nuclear material accounting and control is an important technical means of domestic nuclear material control, and an indispensable link to support the implementation of bilateral agreements or multilateral international obligations.

At present, our commercial spent fuel reprocessing plant has insufficient experience in accounting and control of nuclear materials, and technology needs to be improved urgently. Guidelines, monitoring schemes and review outlines need to be further improved.

This paper systematically investigates and analyses the status of nuclear material control in domestic spent fuel reprocessing plants. This paper investigates the development history, implementation status and experience and lessons learned from the accounting and control measures for nuclear material in foreign commercial spent fuel reprocessing plants, and the evolution of IAEA’s safeguard and supervision scheme for commercial spent fuel reprocessing plants.

The key measurement points of material balance area and physical inventory in typical commercial spent fuel reprocessing plants, the overall design requirements of nuclear material accounting and control measures, on-line process measurement and monitoring, and near-real-time accounting are analyzed. Based on the investigation results and analysis, and in view of the present situation of nuclear material control in China, some preliminary suggestions are put forward for the preparation of nuclear material control technology for commercial spent fuel reprocessing plants in the future. Including the accounting and control of nuclear materials should meet various requirements, promoting the preparation of accounting and control supervision of commercial spent fuel reprocessing plants, and the accounting and control measures of nuclear materials should be embedded in the overall design requirements of the project, so as to achieve three simultaneous , etc.

State
China

Gender
Female
Primary authors:  CHU, quanlichu; ZHANG, tianbao
Presenter:  CHU, quanlichu
Track Classification:  PP: Nuclear material accounting and control
“Security in the Civil Nuclear and Aviation Sectors – What can they learn from each other?”

The World Institute for Nuclear Security has conducted a major benchmarking research project comparing the evolution and future security challenges faced by the civil nuclear and aviation sectors with the purpose of identifying transferable best practices between them. This paper will provide a summary of the overall conclusions of the research which will be published at the end of 2019.

On first inspection one might ask what these two sectors have in common and why benchmarking their security arrangements is at all relevant.

On the one hand, commercial, civil aviation is a very public activity, transporting billions of people each year between airports. It is a highly dynamic and competitive international sector, where time is money, and where customer satisfaction is a high priority. On the other hand, nuclear power plants (and associated fuel cycle facilities) are some of the most robust, static structures on earth with control points that prevent unauthorised public access. Security at these plants is often characterised by the phrase “guns, guards and gates”; in strong contrast to the public image that airports are trying to achieve.

Yet there are some very important similarities between these sectors. The first is in the way that they are “supervised” by the international community. Both of these sectors are overseen by UN-affiliated international organisations (the International Atomic Energy Agency – IAEA, and the International Civil Aviation Organization – ICAO) comprising their Member States, though neither of these organisations has security mentioned in their founding Statutes.

Both sectors have competent authorities (regulators) that are responsible for national regulations within the international frameworks of standards, recommendations and guidance. Both sectors are considered part of a State’s critical national infrastructure, and both sectors are of concern politically and publicly in respect of possible terrorist attacks. And of course, operators in both sectors would say that their number one priority is “safety and security”, in what need to be high reliability organisations.

The research study has comprised a comprehensive analysis of the publicly available information on aviation and civil nuclear security - both the IAEA and ICAO publish extensive information as do the various trade associations that represent the aviation and, to a lesser extent, the civil nuclear sector. However, in the case of nuclear security, this is supplemented by the work of a significant number of non-governmental organisations that monitor and comment publicly on the work of the IAEA and the state of global nuclear security generally. WINS has also worked with experienced practitioners in both sectors and interviewed countless individuals with responsibilities for aviation and nuclear security, at all levels.

Taken together, this research programme is the most comprehensive effort ever undertaken to benchmark security in these critical sectors, and to identify root causes for any differences and opportunities for cross-sector improvement. Subjects covered include:

- A comparative analysis of the civil nuclear and aviation sectors, the threat landscape and analysis of events and incidents over the last 50 years,
- The role and evolution of the IAEA and ICAO in establishing security guidance, recommendations and standards, and their interface with key stakeholders, including industry,
- The implementation of international security recommendations and standards,
• The IAEA and ICAO technical support programmes for security (i.e. IAEA Integrated Nuclear Security Support Plans – "INSSPs" – and the ICAO “No Country Left Behind” programme),
• International peer review and audit for aviation and nuclear security,
• Comparative approaches to security training, professional development and capacity building,
• The development and sharing of best operational security practices within the two sectors,
• The development of Security Management Systems, regulatory approaches and the interface between safety and security,
• A comparative analysis of how insider threats, human reliability programmes and cybersecurity are being addressed in the two sectors, and
• Future challenges and issues for security in the aviation and nuclear sectors.

As noted, this paper will provide a summary of the overall conclusions of the research that we believe will lead to demonstrable and sustained improvements in security in both sectors and at all levels, for the benefit of civil society.

State
Austria

Gender

Primary authors: Dr HOWSLEY, Roger; Ms DELGADO, Raquel

Presenter: Dr HOWSLEY, Roger

Track Classification: CC: Advances in nuclear security research and development; international cooperation on nuclear security research
Cross-checking accounting and transportation data: a systematic action towards security

IRSN is the French Technical Support Organization in nuclear and radiation risks and its activities cover all the related scientific and technical issues. Among these numerous activities, it carries out the centralised accountancy of nuclear materials as part of the control of these materials under the authority of the Ministry of Energy (MTES). Within the context of the national regulation, a daily report for any inventory change has to be transmitted to the centralised accountancy by the authorized operators. The centralised accountancy processes every working day the accounting records sent by all the facilities in the country. These records include a lot of information such as the accountancy zone in which the activity occurred, type of nuclear material, characteristics and quantities, etc. By crossing this accounting information, a computerised system verifies the validity of the data and their consistency (e.g. matching of the accounting data between shipper and receiver, availability in stocks, respect of international obligations). The data are if necessary, corrected by the operators and lead for each accountancy zone to monthly accounting reports.

IRSN supports also the Ministry of Energy in the management and monitoring of nuclear materials transport with the so-called Echelon Opérationnel des Transports (EOT) which is the French nuclear material Transport Control Center. Prior to the authorization of any transport and during the transport, data describing the nuclear material are requested by EOT pursuant to the national regulation. These data are recorded in a specific database dedicated to transport activities. It is then possible to cross-checked the transport data with those of the centralized accountancy in order to identify any inconsistency. Errors, irregularities or omissions can thus be detected in declarations, deterring malevolent actions. Ways for efficiency improvement and reinforcing the methodology are being considered: creation of a unique common key clearly identifying the material's shipment in the two distinct databases (accounting and transport) and providing of a valuable reporting. As a matter of fact, a specific field identifying the transport "ID" on the accounting report daily transmitted to the centralized accountancy could be used to create a direct link to the transportation database. In addition, a valuable reporting with possibility of sorting will help harness the wealth of numerous available data and shorten the processing time.

State

France

Gender

Male

Primary author: LANAVE, François (IRSN)

Presenter: LANAVE, François (IRSN)

Track Classification: PP: Nuclear material accounting and control
Security regulation overview for radioisotopes in Korea

Radiation is being used widely in industrial, medical, research and education field in Korea. The number of license in Korea have been increased continuously and about 8,500 licenses are valid in 2019. Among them, the number of sealed source user is about 2,400 and about 11,000 sealed sources have been being used.

Legal system was launched in 1953 for radiation safety. Nuclear Safety Act (NSA) is based on IAEA BSS (1996). Basic requirements are including licensing processes (review & inspection) and radiation protection for safety and security.

Security was ancillary measure for safety in the former version of this act. But, introducing new requirements in 2015 based on IAEA security recommendations and code of conduct on the safety and security, the act have got well organized security measures.

Basic security is adopted all radiation handling for prevention of loss and robbery. And special requirements are added for high risk radiation sources such as category 1, 2 of IAEA categorization. These requirements are including security system (based on the concept of detection & assessment, delay and response, etc.) and management (preparation of a security plan, security zones, access control, trustworthiness, information protection etc.)

About 160 licensees are having category 1, 2 radiation sources such as Co-60, Cs-137, Ir-192 for medical or industrial purpose in Korea and each licensee is implementing security measures based on own security management plan.

National level efforts are implementing also. The regulatory authority (Nuclear Safety and Security Commission & Korea Institute of Nuclear Safety) is checking status and encouraging security strengthen. Korea have expressed support for Code of Conduct on Safety and Security of Radioactive Sources including Guidance on the Import and Export of Radioactive sources since 2004. Korea was inspected International Physical Protection Advisory Service(IPPAS) of IAEA in 2012 sucessfully and adopted IAEA security requirments to legal system by publishing 'Requirements for radioisotope security management' in 2015.

Regulatory review and annual inspection to licensee is general activity for security implementa- tion. But special activities were carried when national events were held such as U-20 FIFA soccer games in 2017 and 2018 Pyeong Chang Olympic winter games in order to prevent malicious use. Korea have been making an effort to establish and implement security policy and is going to improve consistently. These efforts are going to contribute spread of security culture.

State
- Republic of Korea

Gender
- Male

Primary author: Dr HAN, Sang eun
**Presenter**: Dr HAN, Sang eun

**Track Classification**: CC: National nuclear security regulations
Evaluation of the Effectiveness of Physical Protection System for Nuclear and other Radioactive Materials Used in Research Institutes

Monday, 10 February 2020 11:45 (15 minutes)

Small quantities of nuclear and other radioactive materials are used in educational institutions worldwide in education, research, health care, agriculture and industry. In practice, it is often desirable to protect the critical infrastructure (buildings, materials and equipment) from malicious acts caused by humans and the protection is usually provided by complex Physical Protection System (PPS). The PPS is a security system which integrates people, procedures and equipment for the protection of assets against theft, sabotage or any other malicious acts. It is designed to achieve a set of objectives according to a plan and must be analyzed to ensure that it meets the objectives of physical protection. The objective of the study is to create an Adversary Sequence Diagram (ASD) and evaluate the PPS effectiveness for the Most Vulnerable Path (MVP) into the research laboratory. The effectiveness of PPS (PE) is the metric for a PPS performance and it is defined as the product of two probabilities: Probability of Interruption (PI) and Probability of Neutralization (PN). The value of PI can be determined by a software namely, Estimate of Adversary Sequence Interruption (EASI). The detection and delay components of the PPS, along with the respective value of Probability of Detection (PD), mean delay time (tD), and Probability of Communication (Pc) are measured along a specific adversary path and are used as inputs in the Adversary Sequence Diagram (ASD). The Response Force Time (RFT) is used to decide the Critical Detection Point (CDP) in the ASD. The CDP is defined as that point along the path to the target, detection beyond which might result in the success of the adversary. The estimation of PN requires data on the threat and the response force. Threat data include threat type, number of adversaries and their capabilities and a specific target. The response force data contain the information about weapons, number of guards and response time for each target. In the present work, the evaluation of PPS designed for a research laboratory in a university campus against sabotage is presented. Adversary’s intent is to reach the radioactive material storage vault in the research laboratory and conduct sabotage. The analysis includes the path travelled by the adversary from fence or gate (off-site) to the target through various detection and delay elements of the PPS. The assumed RFT is 110 seconds and PC is 0.95. The CDP is set at 133 seconds at the lab door. The calculated value of PI is 0.98. The high value of PI represents that adversary’s success probability will be very small if they attack through this path. For the PN calculation, we assume adversary is an insider with a pistol. The response force includes one watchman with pistol and two persons in alarm response team. With these inputs the value of PN = 0.96. Therefore PE will be 0.94 i.e. the PPS is 94% effective. So, the effectiveness of the PPS at a research laboratory in a university campus is evaluated by estimating PI and PN. The considered sabotage scenario and the evaluation of the PPS effectiveness serve as an academic exercise which was found useful to demonstrate to the students about how PPS evaluation can be done.

State

India
Gender

Female

**Primary authors:** Dr KALRA, Kawalpreet (Amity University); Prof. GOEL, Alpana (Amity University); Prof. S. CHIRAYATH, Sunil (NSSPI, Texas A & M University)

**Presenter:** Prof. GOEL, Alpana (Amity University)

**Session Classification:** Physical protection systems: evaluation and assessment

**Track Classification:** PP: Physical protection systems: evaluation and assessment
Acquired Experience in the use of National Radiological Incident Database in Chile Period 2013-2018

Introduction:
Chile has been one of the first countries to integrate the use of the Incident and Illicit Trafficking Database of the International Atomic Energy Agency, ITDB-IAEA. This poster is a study of the descriptive statistical analysis of the National Database of Notifications of Radiological Incidents in Chile, BADNIR.

Goals:
Evaluate the present situation, patterns and trends in the use of BADNIR.

Method:
The data of the forms of Notification of Radiological Incident R2 and R24 of BADNIR-Chile, between the years 2013-2018, were collected. From the descriptive statistical analysis of BADNIR, based on tables and graphs, it will be possible to visualize the current status of the radiological contingencies, and to make a diagnosis of the radiological events that occur in Chile, indicating, especially, what type of materials are reported, including those that are outside regulatory control and radioactive sources that have not yet recovered.

Results:
In the period of the last five years, there were 54 notifications of radiological incidents, broken down into 3, 8, 15, 10, 7 and 11 per year, respectively; the records include the incidents by region, city and commune, if it is an interior country or border, place of occurrence, type of incident, material type of scrap and equipment involved. In particular, we have: Nuclear density meters (91%), Ba-133 density meters (3%), gammagraphy equipment (3%), X-ray equipment (3%); equipment not recovered (61%); cases of radioactive material involved: Cs-137 (29), Am241 (Be) (26), Ba-133 (1), I131 (1), Iridium192 (1), Depleted Uranium (1) and Co-57 (1) . The largest number of notifications sent to the ITDB-IAEA was the year 2015, with 11 reports, and the year 2018, with 8 reports; most of the thefts of equipment with radioactive sources occurred during transport, representing 86% of the cases, following from the storage warehouse; the findings occur, mainly, in the public thoroughfare, as a consequence of the campaign of diffusion in the press and television about the danger and risk of lost or lost nuclear or radioactive equipment; the majority of robberies occurred in the Metropolitan Region (57%); most of the findings occur in the Metropolitan Region (67%); of the eleven (11) Unrecovered equipment, nine (9) are from the Metropolitan Region, one (1) from the Coquimbo Region and another (1) from the Los Lagos Region; of the equipment not recovered ten (10) were Nuclear Densimeters that contain radioactive sources of Cs-137 and Am-241; the other type of lost densimeter contains a radioactive source of Ba-133; of the equipment not found, 82% corresponds to the Metropolitan region, corresponding 91% of them Nuclear Densimeters. Since some of the radioactive sources remain active in years, thousands of years and millions of years, their recovery is necessary as soon as possible, in order to remain under regulatory control.

Conclusions:
Ensure the continuity of notifications of radiological incidents, the inspection during transport of equipment with radioactive sources and the judicial investigation to recover the stolen materials, attending to their activity for hundreds, thousands and millions of years, and the institutional coordination between the national authorities competent. Consequently, the prompt recovery of equipment with radioactive sources, as well as the State’s control actions, must be strengthened, in order to avoid damage to people, the environment, as a result of possible malicious or malicious use, and to avoid the economic impact that would mean an accident with a radioactive and / or nuclear source, normally of high cost.

Discussion:

May 9, 2020
The information contained in the National Database of Radiological Incidents gives an account of the national situation, broken down by regions of the country; its analysis allows the identification of trends and common patterns of the loss of regulatory control of radioactive sources and nuclear material. Consequently, it allows to evaluate the threats and weaknesses of the national nuclear security; keep updated the basic threat of the design of the physical security of a nuclear installation (DBT), and is a great support for the development of the commitments acquired with the implementation of the Resolution 1540 of the United Nations.

The analysis shown in this Poster suggests the construction of tables and graphical types such as those presented by the ITDB-IAEA, in order to produce statistics at the national level, and to compare the situations that have occurred between neighboring countries and worldwide. The need for each state to design a database with common items, according to their needs, is made visible. The items in the Database should contain: correlative number of events, date of the event, place, type of source, sealed or open source, Isotope and its activity, area of the incident, brief summary of the incident; indication of the brand, model, serial number and year of the damaged equipment and its radioactive source, category of the national radioactive source and IAEA; if it was recovered, recovery date, and if the event was informed to the ITDB-IAEA, among others.

**State**

Chile

**Gender**

Male

**Primary author:** Mr FINSCHI, Eugenio (Nuclear Energy Chilean Commission)

**Presenter:** Mr FINSCHI, Eugenio (Nuclear Energy Chilean Commission)

**Track Classification:** CC: Information exchange for incidents of nuclear and other radioactive material out of regulatory control
Application of a simplified five step process to identify and classify Sensitive Digital Assets

Monday, 10 February 2020 12:30 (15 minutes)

The identification of digital assets and their classification (i.e., assignment to security levels) within computer security programs at nuclear facilities has historically been a complex process. The current approaches use a system or asset-centric approach with the aim of applying cyber-security retroactively. An example of such an approach is provided in US NRC Reg Guide 5.71 [1] whereby Licensee systems are classified as critical systems if they meet one or more of the following criteria: (1) Performs Safety, Security or Emergency Preparedness (SSEP) functions; (2) Affects critical systems, functions or pathways; or (3) Supports critical systems.

This paper outlines a simplified approach for identification and classification of digital assets, and provides opportunities to identify strategic improvements and efficiencies in achieving the computer security goals. The paper outlines a 4-element process: (1) identify and enumerate the nuclear security goals; (2) identify the functions that provide, support, or assist in realizing the security goals; (3) identify the digital assets (or systems) that perform or support these functions; (4) assign a computer security level to the digital assets upon the potential consequence as well as the level of support the digital asset provides (i.e., directly performs function, supports function, or indirectly supporting function/auxiliary); and (5) evaluate the effects of compromise using an adversary profile and characterization.

The paper will provide a description of key steps stressing the importance of security by design that is encapsulated in elements (1) through (4) above. The objective of these steps is to establish a baseline using analysis of facility systems and digital assets that perform or support functions that are important to achieving security goals. This analysis can lead to highly accurate outputs that justify assigning a high degree of confidence to the identification and classification. This approach mirrors with safety analysis as the threat is not considered, simply the security goals that are achieved through the provision of functions.

No matter how capable the team performing the analysis, or how accurate the results are, compromise of digital assets can lead to indeterminate effects (ref NSS 33-T). Indeterminate effects reduce the confidence in the functional analysis that dominates elements (1) to (4), and necessitates element (5). The process for element (5) is to bound the potential for compromise resulting in indeterminate effects to those that are bound to an adversary profile and to a credible scenario. This process will never be as accurate as the results of analysis of (1) to (4) since both the scope bounding the adversary and the credible scenarios will not have high confidence, but when used to verify element (4) it is effective. The paper argues that (4) should only be used to confirm the assignment of a security level or raise the level, it should not be used to lower the level.

References:

State
Canada

Gender
Male
Primary author: ROWLAND, Michael (Practical Reason Incorporated)

Co-authors: Mr SLADEK, John (John Sladek Enterprises Inc.); STJOHN-GREEN, Mike (Mr); ANDERSON, Robert (Idaho National Laboratory)

Presenter: ROWLAND, Michael (Practical Reason Incorporated)

Session Classification: Identification, Classification, and Protection of Digital Assets in a Nuclear Security Regime

Track Classification: CC: Information and computer security considerations for nuclear security
Evaluation of the appropriateness of Trust Models to specify Defensive Computer Security Architectures for Physical Protection Systems

Defensive Computer Security Architectures (DCSA) are a vital element in the application of computer security to nuclear facilities. The DCSA should provide higher degrees of protection to digital assets performing more significant functions. This will increase the difficulty to the adversary as they will need to overcome multiple, diverse, and independent measures to successfully complete an attack.

Basing the DCSA specification on a well-established trust model, allows for effective application of good computer security practices in. Current US Regulation mandates a trust model similar to Biba which prioritizes reliability (e.g. integrity and availability requirements) over confidentiality. This leverages the existing Nuclear I&C architecture for safety which allows for measures such as data-diodes, and restrictive procedures (such as requiring independence and channelization) to be put into place. Implementing a DCSA can be very effective against a cyber attack that could result in sabotage potentially leading to unacceptable radiological consequences (URC).

Current DCSA and its underlying trust model does had not been applied sufficiently to physical protection systems (PPS) where the current practice is to assign all devices to a single security level and apply a 'large zone' around all the components of the PPS. This requires extra effort to physically protect networks and components, as well as provide administrative controls to control access.

PPS contain both personally identifiable information (biometrics) and other confidential information as well as have to operate reliably. With these requirements on the system, the trust model in use for Nuclear I&C (Biba), with its emphasis on integrity and availability is unsuitable.

This paper will aim to propose use of well-established trust models to apply to the DCSA specification for PPS. The trust models to be considered are (1) Biba; (2) Bell-LaPadula; (3) Clark Wilson; and (4) Brewer and Nash. The comparison will (1) identify significant functions performed and/or sensitive data managed by an example PPS; (2) identify the underlying tasks or activities that are required to be successfully achieved to delivery the security function or to protect the data (information); (3) indicate the priority of the Confidentiality, Integrity and Availability (CIA) requirements for each task; and (4) for each task, evaluate each trust model as to whether the information flows they allow are effective or ineffective in providing security.

State

Canada

Gender

Male

Primary author: Mr SLADEK, John (John Sladek Enterprises Inc.)
Co-authors: ROWLAND, Michael (Practical Reason Incorporated); NICKERSON, Charles (Idaho National Laboratory)

Presenter: Mr SLADEK, John (John Sladek Enterprises Inc.)

Session Classification: Identification, Classification, and Protection of Digital Assets in a Nuclear Security Regime

Track Classification: CC: Information and computer security considerations for nuclear security
The relationship between Maturity and Regulatory Models (Prescriptive vs. Performance Based) for Cyber Security

In February 2013, US President Barack Obama, promulgated Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity", in which he directed the National Institute of Standards and Technology (NIST) to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure [1].

In response, NIST released its Cybersecurity Framework for use across all critical infrastructure sector on February 12, 2014 [2] which was revised on April 16, 2018 [3]. "The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization’s risk management processes. The Framework consists of three parts: the Framework Core, the Implementation Tiers, and the Framework Profiles [3]."

The debate currently is how best to apply this in a heavily regulated sector, like that in which nuclear power plants operate. Three central questions require detailed consideration: (1) What is the role that the State and the competent authority play in progressing both competence and capabilities of licensees? (2) What type of regulation (prescriptive or performance-based) is most appropriate based upon both the organization and human resources available within the State? and (3) how is risk identified, assessed, evaluated and treated by both the State and the licensee? This paper contemplates these questions and proposes potential directions and actions to cultivate maturity of organizations using the NIST framework as a reference. The focus will be on the transition from establishing a foundational level of maturity using a prescriptive based approach to an adaptive level of maturity relying upon performance based approaches.

References:

State
   United Kingdom

Gender
   Male

Primary author: STJOHN-GREEN, Mike (Mr)
Co-author: ROWLAND, Michael (Practical Reason Incorporated)
Presenter: STJOHN-GREEN, Mike (Mr)

Track Classification: CC: Information and computer security considerations for nuclear security
Machine Learning -based process control monitoring and cyber security: Similarities, conflicts and limitations

Analog control systems are being replaced by digital Instrumentation and control systems in the nuclear power plant control consoles to improve reliability, availability and enhance the decision-making process. The introduction of digital systems has produced a network of reactor safety components with Programmable Logic Controllers (PLCs), sensors, valves, and breakers. By association, the vulnerabilities in these digital systems have been inadvertently transferred to the safety systems and these cyber vulnerabilities could quickly become safety issues. Consequently, when a plant goes into crises mode, the swift response of the operator is highly desirable. In nuclear plants, two most commonly cited causes of abnormality are system faults and cyber attacks. To address these issues, many machine learning abnormality detection techniques have been proposed for a wide range of key systems in nuclear power plants. However, many reported cyber-attacks carried out on process control systems usually appear as system failure or fault injection, and these two “abnormal occurrence” initiating event could sometimes have similar signatures. That is, cyber-attacks could be easily mistaken for a random system fault. It is also observed that, safe for the dataset used in training these machine learning algorithms, the techniques used for fault detection and cyber security are fundamentally similar. In a complex system such as nuclear plant, it is pertinent to develop a robust but distinct detection system with the capability to explore the similarity in signature to differentiate between the two events, as the consequence of each of them, the required response, and the overall effect to system safety are entirely different.

This paper reviews proposed machine learning-based abnormality detection tools, techniques, limitations, issues, challenges and the status of their application in NPP. We also discuss the similarities, conflicts and the limitation of the machine learning tools used for fault diagnosis and cybersecurity in the protection of complex systems such as NPP, and the need to establish clear differences between them. Sources of the dataset used in training and testing the machine learning algorithm are described and their limitations are discussed. Some proposed methodology to integrate security algorithms to enhance safety tool to include malicious attack detection in NPP is also reviewed. Finally, future direction and recommendations for the efficient distinction of these incidences are presented.

State
China

Gender
Male

Primary author: Mr AYODEJI, Abiodun (Nigeria Atomic Energy Commission/Harbin Engineering University)

Co-author: Prof. LIU, Yong-kuo (Harbin Engineering University)
Presenter: Mr AYODEJI, Abiodun (Nigeria Atomic Energy Commission/Harbin Engineering University)

Track Classification: CC: Information and computer security considerations for nuclear security
Strengthening Legal Framework for the Role of BAPETEN’s Inspector for the Law Enforcement and Nuclear Security Inspection

Abstract:
According to the Law Number 10 Year 1997 the main tasks of the Indonesian Nuclear Energy Regulatory Agency (BAPETEN) covers developing the regulation, issuing the license, and conducting the inspection. The implementation of inspection is to conduct law enforcement in the nuclear safety matters. However, the law enforcements are merely for any violations of the absence of the license and/or any administrative matters. For the necessity in the case of nuclear security event and nuclear forensics, it is also important to have the provisions for the law enforcement and nuclear security inspection for any violations regarding to the nuclear security events.

We use juridical empirical methods by emphasizing legislation and regulation aspects to analyze the Law Number 10 Year 1997 on Nuclear Energy, the Law Number 10 Year 2014 on the Ratification of International Convention for the Suppression Acts of Nuclear Terrorism, the Law Number 5 Year 2018 on Amendment of Law Number 15 Year 2003 on Enactment of Government Regulation in lieu of Law Number 1 Year 2002 on the Suppression of Terrorist Act, as the Law, Code of Conduct on the Safety and Security of Radioactive Source, and the Bill of the Replacement of the Law Number 10 Year 1997 on Nuclear Energy. This paper is intended to settle the best solution from legal approach on how to strengthen legal framework for the role of BAPETEN’s Inspector in the law enforcement and combating any violations in case of nuclear security events and nuclear forensics.

We found that the Law Number 10 Year 1997 did not sufficiently regulate for combating any nuclear security events and nuclear forensics. There were not enough authorization for BAPETEN’s Inspector to conduct law enforcement in the case of nuclear security event. For strengthening the legal framework, Indonesia has ratified some international conventions and has obligation to harmonize with national legislation and regulation. Indonesia has ratified the International Convention for the Suppression Acts of Nuclear Terrorism by the Law Number 10 Year 2014. Indonesia has also already signed the Code of Conduct on the Safety and Security of Radioactive Source. The Law Number 5 Year 2018 on Amendment of Law Number 15 Year 2003 on Enactment of Government Regulation in lieu of Law Number 1 Year 2002 on the Suppression of Terrorist Act, as the Law has authorized Badan Nasional Penanggulangan Terorisme – BNPT (National Agency for Combating Terrorism) to combat the terrorist acts. Therefore the nuclear forensics has significant role in the investigation process. However, the Bill of the Replacement of the Law Number 10 Year 1997 on Nuclear Energy was comprehensively developed to sufficiently regulate the provisions of authorization to conduct nuclear security inspection as well as to combat any violations in case of nuclear security events and nuclear forensics. This bill also regulate the authorization of the BAPETEN’s Inspector as Penyidik Pegawai Negeri Sipil – PPNS (Civil Servant as Investigator). It means that the BAPETEN’s Inspector has the same position as police investigator for investigating any violations, both in nuclear safety and nuclear security matters. BAPETEN’s Inspector has also a significant role in the nuclear forensics in the term of coordination in establishing the investigation with the National Police of Republic of Indonesia.

In conclusion, the bill of the Replacement of the Law Number 10 Year 1997 on Nuclear Energy is developed to regulate any provisions to conduct nuclear safety and nuclear security inspection as well as to combat any violations in case of nuclear safety matters and nuclear security events. The bill acts as a national bridge to adopt the International Convention for the Suppression Acts of Nuclear Terrorism.
Nuclear Terrorism into national legislation. The coordination with ministry and/or agency is also an important measure to overcome any obstacles and difficulties in managing the nuclear security events and the nuclear forensics.

**State**

Indonesia

**Gender**

Male

**Primary author:** Mr RUSHARTONO, DWIHARDJO (INDONESIAN NUCLEAR ENERGY REGULATORY AGENCY (BAPETEN))

**Presenter:** Mr RUSHARTONO, DWIHARDJO (INDONESIAN NUCLEAR ENERGY REGULATORY AGENCY (BAPETEN))

**Track Classification:** CC: National nuclear security regulations
NUCLEAR REGULATORY PROGRAMME TO MINIMIZE AND DETER THE POTENTIAL THREAT RELATED TO ILICIT TRAFFICKING

Radioactive Sources are being used all over the world, including Indonesia for many decades to benefit the humankind for various applications. For example to diagnose and treat illness, irradiate food, non-destructive testing, well-logging, etc. Some sources contain relatively large amounts of radioactive material that could potentially be used for malevolent purposes. It is important for Indonesia to prevent, detect and response to incidents involving the illicit trafficking of nuclear material and other radioactive sources.

The Act No.10 Year 1997 on Nuclear Energy stipulated that any activity related to the utilization of nuclear energy is required to be conducted in a manner which observers safety, security, peace, health of workers and the public, the protection of the environment. This requirement is further implemented by Government Regulation No. 33 Year 2007 on Safety of Ionizing Radiation and Security of Radioactive Sources. The aim of the regulation is to ensure the safety, security, peace, and health of the workers and people, and to protect the environment. The Government Regulation No. 33 Year 2007 is based on IAEA BSS 115 and Code of Conduct on The Safety and Security Radioactive Sources. The national strategies to minimize the likelihood of a loss control is based on the Government Regulations Article 60 to article 76. As part of the nuclear regulatory control, an export-import authorization system of radioactive sources are founded in article 61 to Article 65 of the Government Regulation No. 33 Year 2007. Article 61 states that prior to consigning radioactive sources category 1 and category 2, the importer shall ensure that domestic users have already held license from BAPETEN as well as the exporter. Beside, the exportation requires: exporter shall have license from BAPETEN and ensure that importer for radioactive sources category 1 and 2 also holds license from the regulatory authority.

Based on Act 10/1997 on Nuclear Energy, inspection shall be performed by BAPETEN and shall be conducted periodically or timely. Base on Government Regulation No. 29 Year 2008 on Licensing of Ionization Radiation Sources and Nuclear Material, BAPETEN shall perform inspection to verify compliance with regulation or licence’s requirements, executed by radiation safety inspector (assigned by BAPETEN).

The challenges in the regulatory control are due to the geographic position of Indonesia (domestic and international issues), the utilization of radioactive material increase, the lack of infrastructure to monitor and control (fund, inspector, procedure, coordination, etc.), and the fact law enforcement mechanism for non-compliance have not established or implemented. In order to prevent and deter illicit trafficking, Indonesia has installed of radiation protection monitors (RPM) in some ports.

Pertaining to the regulatory control of radiation safety and security, BAPETEN has successfully established an information system on licensing and inspection for radiation facilities and radioactive sources. This model called B@LIS (BAPETEN Licensing and Inspection System) is the Nuclear Energy Regulatory Information System which is operated by BAPETEN. The main objective are to support the licensing process and the inspection activities the utilization of radiation facilities and nuclear installation. In order to control export and import of nuclear material and/or, Indonesia has implemented Indonesia National Single Window (INSW) to prevent illicit trafficking.

REFERENCES

[1.] Act of the Republic of Indonesia Number 10 of 1997 on Nuclear Energy.
[3.] Government Regulation No. 29 Year 2008 on Licensing of Ionization Radiation Sources and
Nuclear Material (2008)


State

Indonesia

Gender

Female

Primary author:  Mrs UTAMI, SRI BUDI (Nuclear Energy Regulatory Agency (BAPETEN))

Presenter:  Mrs UTAMI, SRI BUDI (Nuclear Energy Regulatory Agency (BAPETEN))

Track Classification:  MORC: Preventing illicit trafficking of nuclear and radioactive material
Implementation of the CPPNM and its Amendment into Czech Legislation

The Czech Republic has a long-standing tradition in peaceful utilization of nuclear energy and ionizing radiation. Like other countries, the Czech Republic is also facing new modern ways of threat, especially due to increase of international terrorism, cyber threats, or new affordable technologies that can be misused to steal nuclear material or to sabotage nuclear facilities. Especially insiders pose a significant threat to nuclear security and becoming an important topic within the national and also international community. The Czech Republic is aware of the necessity of international cooperation in this area and ratified the Convention on Physical Protection of Nuclear Materials (CPPNM) and its 2005 Amendment and recently significantly strengthened its legal framework in the field of nuclear security and also nuclear safety.

In the Czech Republic, the new Act No. 263/2016 Coll., The Atomic Act, entered into force on 1 January 2017. This act became a comprehensive codex of public nuclear law. Atomic Act is a piece of legislation that encompasses nuclear safety, radiation protection, radioactive waste management, shipments of nuclear materials and other radioactive sources, security of nuclear materials and nuclear facilities, radiation emergency management, radiation monitoring and non-proliferation of nuclear weapons. The Atomic Act replaced the old Act No. 18/1997 Coll. in which only provisions dealing with civil liability for nuclear damage are still in force. This paper aims to describe new legislation in the area of security of nuclear material and nuclear facilities in the Czech national law which is an integral part of this recodification.

Amendment to CPPNM (which entered into force on 8 May 2016,) meant significant change to the scope of CPPNM. During preparatory drafting work on the aforementioned Czech atomic act, this amendment of CPPNM (apart from other international binding and non-binding documents) was earnestly taken into consideration. Main objective of this paper is to describe how were the particular provisions of CPPNM and its Amendment implemented into the Czech legislation – mainly into the Atomic Act. In addition to that, the Atomic Act was complemented with its detailed implementing Decree of the State Office for Nuclear Safety No. 361/2016 Coll., On Security of Nuclear Material and Nuclear Facility.

Furthermore, there are even more relevant legislative documents in the Czech national law. Respective criminal offences from CPPNM and its Amendment were implemented into the Act No. 40/2009 Coll., Criminal Code, or principle of confidentiality was implemented into the Act No. 412/2005 Coll., On the Protection of Classified Information and Security Eligibility.

But what were the most significant changes in the area of nuclear security in Czech national law? The Czech new Atomic Act, in contrast with the previous one, changed the institute of design basis threat (when the Atomic Act now explicitly states that the method of ensuring physical protection of nuclear installations and nuclear material shall correspond to the hazards arising from the design basis threat which is legally binding resolution of the State Office for Nuclear Safety), performance of sensitive activities and also newly regulates the security of nuclear material not classified in the categories. Significant change in legal obligation of operators of nuclear installations is represented by the new restricted and controlled area – the vital area. There also new provisions that introduce two-person rule or prevent landing of any means of air transport on the roof of nuclear facilities. Interim provisions of the Atomic Act gave recipients of these obligations two years to adapt their facilities and respective documentation to this Act.

All of these changes were based on the CPPNM and its Amendment and relevant IAEA recommendations and this paper tries to describe if and how were the certain provisions of international documents implemented.
State
   Czech Republic

Gender
   Male

Primary author:  KLOBOUCEK, Eduard
Presenter:  KLOBOUCEK, Eduard

Track Classification:  CC: National nuclear security regulations
IAEA’s Technical support for Establishing Requirements for the Security Up-Grades at Egypt’s Second Research Reactor Complex

Monday, 10 February 2020 14:30 (15 minutes)

Abstract
The International Physical Protection Advisory Services (IPPAS) mission has been conducted by IAEA for the Egyptian Atomic Energy Authority (EAEA) in December 2005. The purpose of the IPPAS has been to provide advice and assistance to strengthen the effectiveness of the physical protection systems of Egypt’s second research reactor (ETRR-2) nuclear complex. The purposes of that work is to development and finalize an action plan for the technical upgrade of the physical protection system, and contribute in the implementation of IPPAS mission recommendation, of ETRR-2.

The main objective of this paper is to introduce the upgrading process of the physical protection systems at ETRR-2 nuclear complex, the work determines and recovering for the weakness points in security systems on site and insure the sustainability of the physical protection system to verify; it meets the Regulatory and IAEA requirements.

This paper will present the processes and approaches adopted by the Egypt’s second research reactor for inspecting and evaluating nuclear security aspects and interface of inspection with safety

This paper determines the operational requirements for the physical protection system; devices, equipment, and the systems needed to be upgraded as a part of ETRR-2 overall physical protection systems. The paper will explain how to create the statement of work (SOW), which includes the required specification and the system issues; protection, detection, surveillance television, alarm and access control. The works shows the central alarm station management, security grating barriers and entry check-point’s equipment and devices used in inspection deepening on the regulatory requirements.

The work introduces the issues and challenges currently faced and explain the possible solutions. The work presents the techniques and strategy has been used for developing the physical protection systems in order to assist, the second reactor complex, in enhancing its facilities capabilities in nuclear security and improving the nuclear security regimes

Keywords: Central Alarm Stations (CASs), Isolation zone strengthen, Contraband systems, Intrusion Detection system, Access control system

State
Egypt

Gender
Male

Primary author: Dr TOLBA, Amir (Egyptian Atomic Energy Authority, Second Research Reactor
ETRR2)

**Presenter:** Dr TOLBA, Amir (Egyptian Atomic Energy Authority, Second Research Reactor ETRR2)

**Session Classification:** Physical protection systems: evaluation and assessment

**Track Classification:** PP: Insider threats
A Proposed Design for: Security Lighting and Cameras Surveillance System for Optimum Supervision at a Perimeter Area

Abstract
In this work a proposed design for security lighting and cameras surveillance system for optimum supervision at a perimeter area of a hypothetical nuclear facility will be presented. A perimeter area has an isolation zone between double fences which are surrounds a nuclear facility site. The illumination poles, lamps type, towers space distance and lighting level, required for camera surveillance system will be computed and determined.

The work provides the requirements of cameras surveillance system at nuclear reactors isolation zone. Width of images sensitive area, lens focal length, lens format and angel of view will be determined by calculation method. The work determines cameras type, distributions, camera’s parameters and formulas according to the physical protection design process. The output results will be analyzed and tabulated.

Keywords: Security lighting, Illumination, Perimeter Area, Cameras Surveillance System

State
Egypt

Gender
Male

Primary author: Dr TOLBA, Amir (Egyptian Atomic Energy Authority, Second research reactor ETRR2)

Presenter: Dr TOLBA, Amir (Egyptian Atomic Energy Authority, Second research reactor ETRR2)

Track Classification: PP: Research reactor security
If it is not secure, it is not safe

The first reported cyber-attack on a Safety Integrated System demonstrates that systems important to safety need cyber security measures to avoid their safety arguments being invalidated. But there is a broader justification: cyber security risks arise as a direct result of the nature of networked digital technology, which renders existing safety analysis inadequate to mitigate those risks. Existing standards recognise that safety and security practices need to work together but detailed, procedural best practice is not yet mature. This paper identifies some specific areas where industry thought-leaders could share how they are dealing with this topic and raises a question about the ethics of using of the most advanced networked digital technologies in systems that are important to safety.

State
United Kingdom

Gender
Male

Primary author: STJOHN-GREEN, Mike (Mr)
Presenter: STJOHN-GREEN, Mike (Mr)

Track Classification: CC: Information and computer security considerations for nuclear security
The Benefits of Drone in Transporting Short Half-life Medical Isotopes

Short half-life medical isotopes, such as Mo-99 are widely used in medical application for body diagnoses. The technology of transporting Mo-99 with half-life of 66 hours is very important to develop. The delivery system also must be efficient and quick enough to supply hospital demand, so the activity of Mo-99 when the package arrive still high. The automation capability of drone technology is suitable for this problem because it can accelerate distribution time of Mo-99 to the consumer. The drone technology also can deliver the Mo-99 to remote area so the body diagnoses technology can reach wider community with every life condition. Otherwise, for transporting medical isotopes, drone technology need to be improved continually especially in the security and safety regulation in medical isotopes packaging and drone design.

State

Indonesia

Gender

Male

Primary authors: AWIENANDRA, I Gusti Bagus; Ms ZAINAL, Herlina

Presenters: AWIENANDRA, I Gusti Bagus; Ms ZAINAL, Herlina

Track Classification: PP: Transport of nuclear and other radioactive material: practices, challenges and regulatory issues
Co-60 in scrap metall containers

In January 2019, a shipment containing a highly radioactive Co-60 source was detected in Hamburg in a container of scrap metall imported from Nigeria by a German scrap metal merchant. So far it has not been possible to identify the device the sources stem from, it’s purpose or the design of the machine to determine where it might have originated from.

As more of these sources have appeared in scrap metall in the Netherlands (some of which had a German destination), efforts have been undertaken to get in touch with the Nigerian authorities in order to help investigate the path these sources have taken, especially in light of the fact that the containers were scanned in Nigeria.

In May 2019 Nigeria has requested a fact finding mission to be conducted by the IAEA and within the presentation some of the results of this mission will be presented.

State

Germany

Gender

Male

Primary authors: Dr BOCK, Andrea (BMU); Dr JUNKERSFELD, Jörg (BMU)

Presenter: KROEGGER, Helge

Track Classification: MORC: Preventing illicit trafficking of nuclear and radioactive material
Cyber threats are increasingly one of the major threats facing all countries. The high-profile “ransom-ware” attacks by WANNACRY in May 2017 and the TRITON attack against the safety system at an industrial complex in the Middle East in August 2017, and against a second victim recently, served as reminders that cyber risks are real and increasing. In nuclear facilities including nuclear power plants (NPPs), a cyber attack could knock out digital control systems vital to ensuring the security of plants and materials, to an extent causing physical damages or losing human lives. While many assume that critical infrastructure, including nuclear facilities are “air gapped” and not connected to the Internet, in practice the gap can often be compromised as shown in the STUXNET attack against a uranium enrichment facility.

Faced with this rapidly growing cyber threats, the Center for International & Security Studies at Maryland (CISSM) has developed an “Effect-Centric Approach” to assessing and comparing the cyber-security risks. The approach classifies cyber events to be exploitative or disruptive depending on whether the attack motive is to steal company information to the extent of holding them for ransom, or to interfere with operational functions to the extent of causing physical damages. By evaluating the severities of various cyber events, either within the same attack vector or across different scenarios, the Cyber Exploitation Index (CEI) or the Cyber Disruptive Index (CDI) can be devised, and they can be used by organizations in the public or private sector for assessing and comparing cyber-security risks.

In this paper, we apply the CISSM approach to assess and compare the cyber-security risks for NPPs. The assessment would focus on the attack vectors (scenarios) against the NPP’s digital instrumentation & control system (e.g., the programmable logic controllers and the Supervisory Control and Data Acquisition, etc.) for both safety and non-safety systems; and follow the scenario progresses to their conclusions. Based on the severity of the end-results (e.g., loss of information, ransom payment, damaged equipment, or devastating on-site or off-site radiological releases, etc.), a CEI or a CDI can be devised for these scenarios. The aim is to provide insight for Information-Technology experts, Operational-Technology staff, supply chain vendors, plant managers, organizational leaders, and policy makers for effective communication and threat identification that differentiate the threats from a private problem to a genuine public concern.
**Presenter:** Dr CHOI, Jor-Shan (Lawrence Livermore National Laboratory (retired))

**Track Classification:** CC: Information and computer security considerations for nuclear security
Strengthening the CPPNM Regime through Regular Review Conferences

In 2021, the IAEA will convene the first review conference for the Amended Convention on the Physical Protection of Nuclear Material (CPPNM). The amended CPPNM is one of the most important tools in the fight against nuclear terrorism and is the only legally binding treaty requiring countries to protect nuclear materials and facilities. Article 16 of the amended CPPNM requires the IAEA, the treaty’s depositary, to convene a review conference five years after the amendment’s entry into force. States should use the review conference to create a forum for parties to engage in regular dialogue on how the treaty is being translated into on-the-ground nuclear security progress and to monitor and identify gaps in implementation, review progress, promote continuous improvement, and discuss emerging nuclear threats. Parties can turn the amended CPPNM into a living, breathing tool for dialogue and progress and demonstrate their commitment to building a strong, effective, and sustainable CPPNM regime. The amended CPPNM provides almost no guidance for the review conference, only stating that the review conference will “review the implementation of this Convention and its adequacy as concerns the preamble, the whole of the operative part and the annexes in light of the then prevailing situation.” This minimal guidance allows parties to design a review conference with outcomes that are most likely to achieve the objectives of a strong, effective, and sustainable treaty regime. States should be ambitious and take advantage of this singular opportunity. Perhaps the most important outcome of the 2021 review conference would be a decision to hold regular review conferences in the future with intervals of not less than five years, as allowed by Article 16. Because the terrorist threat will continue to evolve, the treaty must also be dynamic and able to evolve as the security context changes. This will require parties to discuss regularly the treaty’s implementation over time, reflecting, for example, on changes in the threat environment, advances in states’ ability to protect materials and facilities, development of best practices, and emerging technologies. The treaty’s own language—that the purpose of the review conference is to review the implementation of the treaty “in the light of the then prevailing situation”—acknowledges this reality. Continuity of the review process, particularly opportunities for regular dialogue on nuclear security, will enable the treaty to maintain its long-term relevance. This paper provides a rationale for parties to hold review conferences regularly and suggests proposed outcomes to achieve a robust and substantive review conference. It also argues that the amended CPPNM review conference and the IAEA International Conference on Nuclear Security can each provide unique benefits to strengthening global nuclear security.

State
United States

Gender
Female

Primary author: NEAKRASE, Samantha (Nuclear Threat Initiative)
**Presenter:** NEAKRASE, Samantha (Nuclear Threat Initiative)

**Track Classification:** PP: The Amended Convention on the Physical Protection of Nuclear Material review conference in 2021
Analysis of Nuclear Terrorism Threats in Indonesia

According to the International Convention for the Suppression of Acts of Nuclear Terrorism (IC-SANT), which has been ratified by the Government of the Republic of Indonesia into Law No. 10 of 2014, nuclear terrorism is a violation committed if someone uses radioactive material illegally and intentionally to cause: serious death or bodily injury, or serious damage to property or environment, or forcing other people, international organizations or countries to commit or refrain from certain actions. So far, nuclear terrorism has become a global issue.

Indonesia as part of the international community has actively participated in various international cooperation efforts to prevent nuclear terrorism event. Among others is the Nuclear Security Summit forum. Through this forum the Government of Indonesia recognizes the serious threat of nuclear security and the need for international cooperation to achieve the goal of securing all nuclear materials, nuclear facilities, radioactive sources and radiation facilities worldwide from the misuse by various parties.

The Indonesian government acknowledges that terrorism occur lately has increased in their sophisticated method since the perpetrators are able to keep up with technological developments and current community social conditions. Therefore, the acts of terrorism can create fear in the community. In Indonesia, within the period of 2010 to 2017 there were 130 cases of terrorism. This number shows that terrorism is a serious problem in Indonesia which is not only involve domestic actors, but also transnational organizations.

According to Frantz and Collins (2007) nuclear weapons technology is not a new technology that is only owned by the superpower countries. The technology has been found for more than 60 years ago and has become spread and developed worldwide. The simple design of low purity nuclear weapons can easily obtained, especially since the existence of internet. The issue of global nuclear terrorism threats has influenced the Indonesia’s national dynamics strategic environment. The large number of nuclear technology uses in Indonesia, faces with the fact that Indonesia is still facing the terrorism and radicalism threat, this condition may potentially cause Indonesia to face the threat of nuclear technology misuse. In addition, the openness of Indonesia territorial waters and ports due to limited supervision and security control may cause Indonesia to be an illegal trade area which may connected to global nuclear terrorism threats. As an archipelagic country, of the 8.3 million Km2 area of the Indonesia archipelago there are 6.4 million Km2 area covered by ocean, with the coastal line of 108 thousand Km. Therefore, illegal trade activities is a real threat for Indonesia.

In Indonesia nuclear technology has been widely used. There are three nuclear research reactors located in Serpong, Bandung and Yogyakarta, and seven non-reactor nuclear installations located in Serpong. The use of radioactive sources are spread out throughout the Country. Based on data from the Nuclear Energy Regulatory Agency (BAPETEN), as of April 8, 2019, there were 12,039 licenses of radioactive sources and nuclear materials. They are used in medical sector (6,379 licenses), industrial sector (5,641 licenses), and nuclear installation sector (19 licenses). From the perspective of national security, these data indicates potential threats if the radioactive materials are not under control.

Efforts to prevent misuse of radioactive material in facilities are carried out by operators through implementation of nuclear security principles. In addition, BAPETEN applies surveillance and inspection to those facilities. Efforts to prevent the misuse of mobile radioactive sources have challenges since they are more vulnerable to misuse or sabotage. Therefore, to prevent nuclear security event, access to the sources must be selective given to trustworthy personnel. Furthermore, effort to prevent radioactive source illicit trafficking may carried out by installing Radiological Portal Monitor (RPM). Currently, there are six ports installed with RPM.

Having acknowledged those threat, the study focus on analyzing the nuclear terrorism threats in
Indonesia. As an initial study it’s analyze the threat for each province. A nuclear terrorism threat index is used to quantify the threat. The index is calculated from the radioactive sources use and the terrorism incidents. Even though the radioactive sources use may vary day to day, nevertheless the study may give a capture of the threat within the region. Furthermore, future studies are needed to analyze the potential risk impact of the threats as well as to analyze the prevention and deterrence efforts by using currently available infrastructure. The studies are important, since the results are expected to contribute to maintain the Indonesia national security.

**State**

Indonesia

**Gender**

Female

**Primary authors:** Ms APRILIANI, Dewi (Indonesia Defense University); Mr WIJAYANTO, Deddie (Indonesia Defense University); Mr WIDANA, IDK Kerta (Indonesia Defense University); Mr BAWAZIER, Lukman Hakim (BAPETEN)

**Presenter:** Ms APRILIANI, Dewi (Indonesia Defense University)

**Track Classification:** PP: Nuclear security vulnerability assessments
IMPLEMENTATION OF NSS-31 G ON REVIEW OF NUCLEAR AND OTHER RADIOACTIVE MATERIAL SECURITY TRAINING CAPACITIES (BATAN Experience)

Elements of capacity building for nuclear security cover education, training, awareness, workforce management, knowledge management and network management. As an operator, Indonesia National Nuclear Energy Agency (BATAN) has an obligation to ensure adequacy of its capacity building for nuclear security in organization level. According to Implementing Guide NSS-31 G document, one of organization roles in developing its own capacity building programs is to develop strong training programmes, including frequent exercises, to develop and maintain skills and test plans, and to help reinforce the attitudes and behaviours that contribute to a robust nuclear security culture. To do so, BATAN develops nuclear security training scheme for based on level of competency that must be have accordance with position level and personnel responsibilities to nuclear security in the organization. In conducting training program, it is necessary to develop and periodically review a nuclear security training scheme as a framework and clear direction to have an effective capacity building program.

BATAN’s nuclear security training scheme has four level of competencies that are covered in introductory, basic, intermediate and advance training program. Introductory training program provides awareness training for all level of workforces. Basic training program covers mandatory trainings required by Indonesian government regulations and regulatory body. Intermediate training program is designed to fulfil technical knowledge and skills needed by security personnel. Advance training program is dedicated to create nuclear security experts and trainers, to ensure availability of human resources and sustainability of nuclear security training program. Each level of training program has many trainings to conduct.

The training scheme itself had been first introduced in 2014, but it had not been reviewed since that time. Therefore, it is important to do a review after five years of implementation. The review had been carried out by cross-referencing the BATAN nuclear security training capacities with Implementing Guide NSS-31 G document. The document provide guidance needed to develop comprehensive nuclear security training program and capacities for organization level. Output of the review is a matrix of nuclear security training program for BATAN’s workforces and gap of nuclear security capacities in conducting training that should be overcome by BATAN as an organization. As result, several trainings should be added into training scheme and conducted in regular basis. Identified trainings that should be added into training scheme include nuclear forensic for introductory level, security of nuclear and other radioactive material transportation for basic level, maintenance of security equipment, threat and security risk assessment, both for intermediate level and vulnerability assessment for advance level. While, recomendation to fulfil gap in conducting nuclear security training related are establishment of a clear nuclear security training program, development of training curricula, including suitable training methods, provision of training facilities, including exercise field, provision of availability of competent trainer and instructors team and improvement of formal collaboration and cooperation with other training institutions, stakeholders and organization at national and global level.

State

Indonesia
Gender

Female

Primary author: INDRAGINI, Indragini (National Nuclear Energy Agency)

Presenter: INDRAGINI, Indragini (National Nuclear Energy Agency)

Track Classification: CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
The United Nations Security Council Resolution 1540 (UNSCR 1540) in 2004 highlights the legislation phase of the United Nations Security Council. Before the establishment of this resolution, the Security Council Resolutions are interpreted mainly to maintain peace and security towards the existence of international armed conflicts. The mandate to maintain peace and security, as stipulated in Article 24 of the United Nations Charter, is also followed by the power as stated in Article 39 in the Chapter VII of the United Nations Charter. The power given to the Security Council in the latter Article, allows the Security Council to determine whether ‘threat to the peace’ has occurred or not. Since UNSCR 1540, this power has been interpreted in a broader sense. The measures that are taken by the Security Council to maintain or restore international peace and security have now comprised law-making power and as a member of the United Nations, Indonesia is also required to follow the rules and obligations as set forth in UNSCR 1540.

UNSCR 1540 regulates three objects: nuclear, chemical or biological weapons. One of the obligations related to nuclear in the UNSCR 1540 is that States shall adopt and enforce appropriate effective laws which prohibit any non-State actor to manufacture, acquire, possess, develop, transport, transfer or use nuclear weapons and their means of delivery. Furthermore, the Resolution also requires States to take and enforce effective measures to establish domestic controls to prevent the proliferation of nuclear weapons and their means of delivery, including by establishing appropriate controls over related materials.

In Indonesia, the requirement related to the adoption and enforcement of appropriate effective laws has been stipulated by the Indonesian Government in a number of laws and regulations. For example, the Indonesian Government has established Act Number 5 of 2018 on Terrorism which threatens with penal codes the acts of non-State actor to produce, receive, obtain, deliver, possess, carry, supply or own, store, transport, hide, or remove from the territory of Indonesia, nuclear and radiological weapons. There is also Act Number 7 of 2014 on Trade which requires registration of items related to safety, though does not mention nuclear specifically. However, Indonesia is a Non-Nuclear Weapon State and not a member of the Nuclear Supplier Groups (NSG) and therefore there is only small possibility that a non-State actor in Indonesia could manufacture or produce nuclear and radiological weapons. It is more likely that Indonesia becomes the country of transit or trans-shipment of radioactive materials to be used as nuclear and radiological weapons due to its geographical position.

This paper will discuss how to improve export control in Indonesia by taking into account the obligations as stated in UNSCR 1540 in order to recognize the gaps in Indonesia’s export regulations. The methodology used in this paper is publication research and reviews on the existing laws and regulations in Indonesia. This paper will find that some of the requirements from the UNSCR 1540 could be implemented in Indonesia by establishing stringent laws and regulations, especially related to end-user control in order to prevent the possibility of transit and trans-shipment of radioactive materials for possible use of nuclear and radiological weapons.
Indonesia

Gender
Female

**Primary authors:** Ms ARIETHIA, Midiana (Badan Pengawas Tenaga Nuklir); Mr SANYOTO, Aris (BAPETEN)

**Presenter:** Ms ARIETHIA, Midiana (Badan Pengawas Tenaga Nuklir)

**Track Classification:** PP: Transport of nuclear and other radioactive material: practices, challenges and regulatory issues
Nuclear security requirements for control of nuclear material: graded approach

Control of nuclear material is an important part of nuclear security measures. Control of nuclear material can be part of NMAC (nuclear material control and accounting) measures or PP (physical protection) or both. NSS 20 identifies (as part of Essential element 3: legislative and regulatory framework) that the legislative and regulatory framework, and associated administrative measures, to govern the nuclear security regime should (among other things) provide for the establishment of systems and measures to ensure that nuclear material and other radioactive material are appropriately accounted for or registered and are effectively controlled and protected.

NSS 25-G defines that control of nuclear material as part of NMAC have objective to ensure continuity of knowledge, and thereby to enhance the ability to deter and detect unauthorized removal of nuclear material. Control is defined as activities, devices, systems and procedures that ensure that the continuity of knowledge (e.g. location, quantitative measurements) about nuclear material is maintained. At the same time NSS 13 defines that effective access control measures should be taken to ensure the detection and prevention of unauthorized access.

In Russian Federation Federal environmental, industrial and nuclear supervision service (Rostechnadzor) is authority, responsible regulatory activities regarding safety and security of peaceful use of atomic energy. Focus on regulatory activities in nuclear security area is mainly on NMAC and PP.

In regulatory approach it is recognized that NMAC and PP systems are quite separate systems, but complement each other, including measures for control. Need for interaction and cooperation between them recognized and reflected in regulation. There are separate sets of regulations on PP and NMAC in Russia, but, ideas and requirements for their interactions are incorporated in both sets and implemented in practice at facilities. At the same time it should be understood that control measures for NMAC and PP have different objectives: NMAC control focuses on NM and access to NM, while PP control focuses on protected areas (also can be buildings, rooms etc.) and access to them. Some of control measures are required in both NMAC and PP regulations (such as seals and two person rules).

Paper discuss requirements for control of nuclear material in both NMAC and PP regulations, shows differences in such requirements and at the same how their are complement each other in order to have effective comprehensive nuclear security system at nuclear facility.

State

Russian Federation

Gender

Male

Primary author:  BOKOV, Dmitry (Rostechnadzor)

Presenter:  BOKOV, Dmitry (Rostechnadzor)
Track Classification: PP: Nuclear material accounting and control
ENCOMPASSING A SYSTEMIC RESPONSE TO INVESTIGATIONS OF NUCLEAR AND RADIOACTIVE MATERIAL OUT OF REGULATORY CONTROL

The IAEA’s Incident and Trafficking Database (ITDB) compiles 3497 confirmed reports of nuclear and other radioactive material out of regulatory control (MORC) from 1993 to 31 December 2018 to include 253 incidents involving unauthorized acts reported in 2018. Better recording of trafficking incidents, improvements in the resolution of alarms emanating from radiation detection events, and comprehensive plans and preparation for nuclear security management and mitigation are the result of the availability of published guidance, exercises to test national and regional capabilities, comprehensive training, as well as advances in research to facilitate consequence management. Optimized nuclear security practice involves systematic implementation of nuclear security practices across the spectrum of situational awareness of MORC, radiation detection architectures, radiological response to include those involving crime scenes, nuclear forensics to identify the origin and history of MORC as well as resulting investigative leads. Expertise and infrastructure - whether it be radiation detection, evidence collection, or nuclear forensics - implemented in isolation is not as effective as interfaced efforts that promote the systemic response to a nuclear security event.

The challenge for an effective plan to address a nuclear security event involving MORC is to bridge discipline boundaries involving physical science, biological/medical science, engineering, digital science, jurisprudence, political science, information science, and international relations to provide a systemic response. Important is to identify and utilize existing capabilities and expertise within States (to include regulatory authorities, the university, research institutes, industry, medicine, nuclear operators, police, first responders, and relevant ministries). Nuclear security disciplines do not work in isolation. To this end, nuclear trafficking reports inform information alerts, radiation detection informs radiological response, radiological response informs nuclear forensics and nuclear forensics informs an investigation. Awareness maintained across the nuclear security spectrum is the key to the development and sustainability of an effective nuclear security regime given the dynamic and ever-evolving nature of the threat. Actions taken at the scene of a nuclear security event to collect evidence have profound implications for the confidence in the ensuing nuclear forensic laboratory analysis, findings and conclusions. Coordination and cooperation is enhanced through national and regional measures (to include bi-lateral arrangements) that facilitate bespoke and timely solutions where they are needed to prevent and mitigate. Multi-laterally, by exploiting the accomplishments of the IAEA, the Global Initiative to Combat Nuclear Terrorism, INTERPOL, and the Nuclear Forensics International Technical Working Group, and others, information can continue be to effectively shared between the nuclear security scientists, law enforcement, responders and policy makers to prepare for response. Going forward, common applied field, laboratory and table-top exercises, realistic trainings to include nuclear and radioactive materials studied under controlled conditions, cross disciplinary research to improve forensics examinations as well as broader outreach that spans response and investigations are imperatives.

State
Argentina

May 9, 2020
Gender

Male

Primary author: BIEDA, Tomas (Ministry of Energy and Mining)
Co-author: SMITH, David Kenneth (Division of Nuclear Security, International Atomic Energy Agency)
Presenter: BIEDA, Tomas (Ministry of Energy and Mining)

Track Classification: MORC: Nuclear forensics
Promoting a collaborative, sustainable nuclear security culture through multilateral information sharing on counter nuclear terrorist response capabilities

The Global Initiative to Counter Nuclear Terrorism (GICNT) is a voluntary partnership of 88 countries and six international observer organizations that are committed to strengthening global capacity to prevent, direct, and respond to countering nuclear terrorism by conducting multilateral activities that strengthen the plans, policies, procedures, and interoperability of partner nations. The GICNT’s Response and Mitigation Working Group (RMWG) promotes a collaborative, sustainable counter nuclear terrorism culture through multilateral information sharing on counter nuclear terrorism response capabilities. This paper examines the vital importance of multilateral cooperation and coordination before, during, and after a nuclear terrorist attack. In addition, this paper highlights lessons learned and best practices from previous RMWG workshops. Lastly, this paper explains how sustainability is critical to the RMWG’s strategy in fostering a counter nuclear terrorism culture.

As the name suggests, the RMWG focuses on a response capabilities to a nuclear terrorist attack. In the past two years, the Working Group held six workshops with participants from over 50 countries and 3 organizations. Throughout the workshops, multilateral planning and preparation for a nuclear terrorist attack arose as a common theme. To facilitate response in a timely, appropriate manner in order to save countless lives, it is of paramount importance to properly prepare and establish networks within the international community to create a unified response. One mechanism for leveraging international partnerships and information exchange is through multilateral exercises and training; the workshop “Panda Warrior” is just one example of the RMWG’s work in this arena. The workshop, hosted by China, focused on multilateral preparations for major public events and discussed procedures for preventing and responding to a nuclear terrorist attack that if not prevented could cause mass casualties at the event.

The RMWG acts as a venue for partners to share standard operating procedures and best practices on coordination within the international community during a devastating terrorist attack; the Working Group also provides an opportunity for international organizations to identify the types and level of assistance they can provide. To this end, Argentina and Chile hosted a bilateral response exercise “Paihuen II” to identify the standard operating procedures for bilateral coordination. By understanding the types and procedures of international coordination and assistance, countries can ensure they receive the optimum amount of aid during a response.

International assistance extends beyond immediate response, and can further enhance capacity for investigation and prosecution of nuclear terrorist incidents. Through RMWG workshops, such as the regional “Valiant Eagle” workshop in Nigeria, countries and international organizations can discuss the international and national legal frameworks for prosecuting nuclear terrorist incidents. The RMWG events also provide a venue to share best practices for passing legal frameworks through their legal systems and operating procedures for prosecuting a terrorist incident across borders. In addition, international organizations, like INTERPOL and the IAEA, can discuss what investigative and legal assistance they can provide to a country. Through international cooperation and prosecution, countries can ensure terrorists are prosecuted to the fullest extent of the law, thus deterring further terrorists from committing this heinous crime.

Sustainability is as a crosscutting pillar of RMWG’s strategy. The RMWG strives to ensure all
partner nations can implement RMWG’s workshop outcomes in their home countries. A major mechanism for sustainability is the RMWG exercise playbook, which allows countries to use past workshop exercises on a national basis, thus continuing the discussions of policy and best practices within their country. Another mechanism is RMWG’s Fundamentals for Establishing a Nuclear Security Response Frameworks document, which details the important mechanisms of a response strategy and explains how to create one.

**State**
- Argentina

**Gender**
- Male

**Primary author:** BIEDA, Tomas (Ministry of Energy and Mining)

**Co-author:** Mr FOURCADE, Martin (Undersecretariat of Nuclear Energy)

**Presenter:** BIEDA, Tomas (Ministry of Energy and Mining)

**Track Classification:** CC: Emergency preparedness and response and nuclear security interfaces
Project Management Strategy of Physical Protection System Upgrading for Nuclear Facility

Monday, 10 February 2020 17:30 (15 minutes)

This paper introduces the main concepts of the project management strategy for upgrading the Physical Protection System (PPS) at nuclear facilities. The project scope is redesigning the security systems to enhance the security measures to fulfill the requirements and recommendations of IAEA and the vision of the member state. The most challenging of security project is the successful management of project and solving the problems such as lack of resources, budget, and qualified contractors. However, failure in managing project causes waste of resources and delays the closing, which affect the reliability of protection and increase the threat likelihood. This work gives an integrated model for the project phases based on the project management standard and the Project Management Institute (PMI) models.

State

Egypt

Gender

Male

Primary author: Dr ABDELAAL, Magdy (Manager of ETRR-2, EAEA, Egypt)

Presenter: Dr ABDELAAL, Magdy (Manager of ETRR-2, EAEA, Egypt)

Session Classification: Research Reactor Security

Track Classification: CC: Establishing and formalizing nuclear security processes into integrated management systems
Interface between nuclear safety and security in radioisotope production facility

ABSTRACT
Radioisotope production facility is completed and commissioned in 2013 to produce some radioisotopes for medical and industrial applications. Nuclear safety and security is standardized and have common purposes for protection of people, society and the environment. In both cases, such protection is achieved by preventing a large release of radioactive material as well as nuclear material protection. Many of the principles to ensure protection are common, although their implementation may differ. Moreover, many elements or actions serve to enhance both safety and security simultaneously. For example, the containment structure at a radioisotope production facility serves to prevent a significant release of radioactive material to the environment in the event of an accident, while simultaneously providing a robust structure that protects the facility from a terrorist assault. Similarly, controls to limit access to vital areas not only serve a safety function by preventing or limiting exposures of workers and controlling access for maintenance to qualified personnel, but also serve a security purpose by inhibiting unauthorized access by intruders. The purpose of this manuscript is to provide a better implementation and understanding of the interfaces between safety and security procedures in radioisotope production facility. It discusses the means to achieve both objectives interchangeably in an optimal procedure. It also adopts the required actions with the goal of maximizing the protection of the public, property, society, and the environment through an improved and strengthened interfaces between safety and security.

State
Egypt

Gender
Male

Primary author:  Dr ELKHATIB, Hesham (Egyptian Atomic Energy Authority)
Presenter:  Dr ELKHATIB, Hesham (Egyptian Atomic Energy Authority)

Track Classification:  PP: Physical protection systems: evaluation and assessment
Making Australian Nuclear Security Regime Fit for Purpose

This paper outlines the outcomes of reviews and reforms related to licencing elements of Australia’s nuclear security regime. The Nuclear Non-Proliferation (Safeguards) Act 1987 [1] enables the grant of permits to nuclear operators and transporters. Permits specify regulatory requirements and can be tailored to be industry specific. Australia’s application of State level physical protection is consistent with the international nuclear security guidelines for nuclear material and facilities [2]. However, the vast majority of Australian permit holders (licensees) have nuclear material holdings that are below Category III [2]. The elaboration of prudent management practices, applied at State level, led to the expansion of nuclear material categorisation to include a ‘Category IV’ nuclear material holdings for source and special fissionable materials and includes a series of categories for locations outside of facilities. This expanded categorisation allowed for a structured graded approach to physical protection measures, providing for uniform security requirements across industries with similar nuclear material holdings. Australia originally granted individualised permits to possess or transport nuclear material based on a developing security understanding and best practice at the time of issue. This permit format provided for discrete security performance requirements that was suitable for the limited numbers of Permit Holders at the time. However, as the number of permit holders increased, the need to increase efficiency necessitated the streamlining of permits. Starting in 2015, ASNO embarked on a reform of its permit system relating to physical protection and IAEA safeguards, into industry specific classes. Permits not only include the requirements for the protection of nuclear material and equipment, but also include the protection of associated nuclear technologies and information. Giving preference to a performance-based, as opposed to prescriptive-based, approach to compliance, permit formats allow for, and draw on the security maturity of each industry. The new permit classes accommodate for industry and functional differences including transport, mining, facilities, radiographers and other locations outside of facilities, but also address protection of associated nuclear technologies. Each type of permit includes specific limits on nuclear material holdings. So far, 23 permit classes have been established. The new permit format divides the document into a dedicated Permit section and a Compliance Code common to each class of permit. The Permit section includes all the individual Permit Holder’s company details, total nuclear material holdings and includes any approved locations for the use and storage of nuclear material. This section also provides overarching security principles and detailed requirements for State and IAEA inspections. The Compliance Code holds all the physical protection (and IAEA safeguards) requirements that are common to all the permit holders for each class of permit. The level of detail is industry dependant and reflects the practical application of physical security required. To improve regulatory transparency, ASNO has published template versions of most of the permits and corresponding Compliance Codes on its website. By providing online access to permits, guidance material and glossary information, ASNO supports its newly introduced permit holder’s online access portal. This web based platform is an access controlled database for material accounting and transport of nuclear material by permit holders. Australian industry and regulatory terminology do not always align with Agency terms [3][4] and historically ASNO permits and forms have had individualised glossaries. ASNO has developed a general glossary of terminology that strives to increase commonality of terms and limiting terminology conflicts across all permit classes. The glossary includes IAEA specific terms for reference. This paper will expand on the reform process, outcomes, lessons learned and planned actions to further improve the permit system and Australia’s national security regime.
REFERENCES:

[1] AUSTRALIAN SAFEGUARDS AND NON-PROLIFERATION OFFICE (ASNO), Nuclear Non-Proliferation (Safeguards) Act 1987, Australia.


State
Australia

Gender
Male

Primary author: Mr BOTHA, Michal Jacobus (Australian Safeguards and Non-Proliferation Office)

Presenter: Mr BOTHA, Michal Jacobus (Australian Safeguards and Non-Proliferation Office)

Track Classification: CC: National nuclear security regulations
A Data Classification and Analysis System for the Identification of Cyber Security Events in a Condenser and Condensate HIL System

KAERI has built a condenser and condensate HIL system as a part of IAEA CRP J02008 “Enhancing computer security incident analysis and response planning at nuclear facilities.” The condenser and condensate system, which is a simple version of physical feed-water condenser system in nuclear power plants, is integrated with a hypothetical pressurized water reactor simulator “ASHERAH”, which is also developed by other parties in the IAEA CRP. This integrated system is designed and developed for computer security R&Ds and training activities to provide how security technologies and processes can enhance computer security incident response.

In this study, a data classification and analysis system has also been developed and added to the condenser and Condensate HIL system for the collection and analyses of the information generated within the HIL system being operated in conjunction with the ASHERAH simulator. The data classification and analysis system can gather all raw input and output data and store at different resolutions for a security event analysis. Through the analysis of events and the selection of candidate parameters, criteria on the classification of information to identify security events can be defined.

At the same time, the display in the data classification and analysis system is designed with easy-view dashboards for tracking the changes in control and monitoring data. Trend displays on dashboards are used to locate and identify possible symptom of cyber events in the HIL system. This study will continue to be developed and optimized for using IAEA International Training Course in collaboration with IAEA CRP J02008 participants.

State

Republic of Korea

Gender

Male

Primary author: Dr SONG, JAE-GU (Korea Atomic Energy Research Institute)

Co-authors: Dr LEE, JUNG WOON (Korea Atomic Energy Research Institute); Dr LEE, CHEOL-KWON (Korea Atomic Energy Research Institute); Dr CHOI, JONG-GYUN (Korea Atomic Energy Research Institute)

Presenter: Dr SONG, JAE-GU (Korea Atomic Energy Research Institute)

Track Classification: CC: Information and computer security considerations for nuclear security
Reflections on regional training efforts in support of nuclear forensic capability development in South-East Asia

Many countries in South-East Asia are seeking to develop capabilities in nuclear forensics. This is part of an overall strengthening of nuclear security architectures in response to increased use of nuclear and other radioactive materials regionally and globally. As a result, there is substantial demand in the region for training and other capability development support. With over two decades of experience in nuclear forensics, Australia is well placed and frequently sought to provide some of this support. Australia has endeavoured to deliver on these requests; in addition to a desire to enhance security in partner nations, Australia recognises that regional nuclear security promotes national security.

On behalf of Australia ANSTO has provided a range of tailored multi- and bi-lateral training programs to regional partners both independently and in partnership with international bodies such as the International Atomic Energy Agency (IAEA). These programs have utilised a range of training modalities including classroom instruction and practical activities such as table-top exercises and hands-on laboratory and field drills. Nuclear forensics training offered by ANSTO emphasises the importance of leveraging existing capabilities within a nation for the development of a robust and sustainable national nuclear forensic capability.

This paradigm of leveraging existing capabilities is also applied to the delivery of training. Whilst activities are led by a team of dedicated nuclear forensic staff, subject matter experts from across ANSTO who provide technical expertise to the national nuclear forensic capability play a key role in delivering training. Utilising enabling functions within ANSTO such as security, safety, international relations and event management is also critical to the success of these training activities. Further, ANSTO seeks to work with external domestic partners, such as the Australian Federal Police (AFP), to provide the highest quality of activities as well as demonstrate the importance of such partnerships in national nuclear forensic capability development. The Australian Government Department of Foreign Affairs and Trade were the funding body for some training activities.

A comprehensive process of continuous review and improvement is a hallmark of ANSTO’s training activities. Detailed feedback is sought from both participants and trainers, which is incorporated into after-action reports which seek to identify trends and articulate opportunities for improvement in future activities. In repeat implementations of some activities, such as the IAEA’s Regional Training Course on Practical Introduction to Nuclear Forensics, the value of these reports has been clearly evident in the improved quality of both the training delivered and the experience for trainers.

The development, delivery and review of training is a valuable career development opportunity for many ANSTO staff, particularly for the early career scientists who are part of ANSTO’s nuclear forensics team. In addition to developing new skills sets in training, these activities provide a valuable opportunity for scientists to reflect upon and enhance technical capabilities. International training activities also build networks for scientists.

ANSTO is far from the only provider of nuclear forensic capability development activities globally or, indeed, in South-East Asia. International organisations such as the IAEA, INTERPOL, the Global Initiative to Combat Nuclear Terrorism (GICNT) and the Nuclear Forensics International Technical Working Group (ITWG) all have important capability development roles, as do national or regional bodies such as the United States’ National Nuclear Security Administration and the European Union’s Joint Research Centre – and this list is not exhaustive. Key challenges moving forward will continue to be ensuring the most efficient deployment of these many, but ultimately
finite, efforts and achieving consistency in content and messaging whilst still respecting the unique contexts, perspectives and relationships of the various providers and participants.

**State**

Australia

**Gender**

**Primary authors:** KAITLYN, Toole (Australian Nuclear Science and Technology Organisation); BLAGOJEVIC, Ned (ANSTO); KEEGAN, Elizabeth (Australian Nuclear Science and Technology Organisation (ANSTO)); GORALEWSKI, Jack (ANSTO); LEE, Samantha (ANSTO); LOI, Elaine (ANSTO); VAN DE VOORDE, Riley (ANSTO); YOUNG, Emma (ANSTO); HOFFMANN, Emmy (ANSTO); APPERLEY, Miles (ANSTO); BULL, Tegan (Australian Nuclear Science and Technology Organisation)

**Presenter:** BULL, Tegan (Australian Nuclear Science and Technology Organisation)

**Track Classification:** MORC: Nuclear forensics
Nuclear Security Detection Architecture on National Nuclear Security Regulation – Case Study Indonesia

Hermawan Puji Yuwana
h.puji@bapeten.go.id
Nuclear Energy Regulatory Agency of Indonesia (BAPETEN)

Abstract
Nuclear Security Detection Architecture on National Nuclear Security Regulation - Case Study Indonesia. The objective of a nuclear security regime is to protect persons, property, society, and the environment from harmful consequences of a nuclear security event. The wide area of Indonesia’s geographical condition, which consists of islands and waters (archipelagic country) becomes a challenge in conducting regulatory control on the utilization of nuclear energy, particularly from the aspect of nuclear security. The challenges on the oversight of nuclear security aspect become a concern both in the national and international levels if linked to potential acts of terrorism. The nuclear security begin to draw particular attention after an increasing number of terrorism threats increase some example of threats where are possible to occur anywhere with unpredictable time and method. Potential theft of nuclear materials to create IND (Improvised Nuclear Device), theft of radioactive materials to make RDD (Radiological Dispersal Device) and RED (Radiological Exposure Device), or potential act of sabotage both for nuclear facility/installation, and transport of radioactive material or nuclear material. This oversight requires the integration of a nuclear security system and nuclear security measures described in the nuclear security detection architecture. Indonesia has established Radiation Portal Monitors (RPMs) in several main seaports to be used for the screening of individuals, vehicles, cargos or other entities for detection of illicit sources from or to the port. This review aims to determine and identify nuclear security architecture detection in national nuclear security regulation in Indonesia. This review uses literature review methodology through national nuclear security regulation, guidance from other countries, and IAEA publications. Nuclear security detection architecture is a framework that integrates the various technical and non-technical elements necessary to detect the illegal activities of nuclear material and other radioactive sources. Nuclear security detection architecture should be developed based on national nuclear security system or national detection strategy. The hierarchy of nuclear energy regulations in Indonesia is stipulated in Act No. 10 Year 1997. The regulation for nuclear security in Indonesia already exist, both at the level of government regulations (GR) and BAPETEN chairman regulations (BCR). There are two GRs related to nuclear security: GR No. 33 Year 2007 on the Safety Ionizing Radiation and the Security of Radioactive Sources and GR No. 54 Year 2012 on the Safety and Security of Nuclear Installations. At the level of BCR, there are BCR No. 1 Year 2009 on Physical Protection of Nuclear Instalation and Nuclear Material and BCR No. 6 Year 2015 on Security of Radioactive Sources. However the existing national nuclear security regulations in Indonesia may not describe prescriptively and specifically the concept of nuclear security detection architecture. Based on the obtained from gap analysis identification of national nuclear security regulations in Indonesia, there are several considerations to support the development of nuclear security detection architecture in Indonesia, they are (i) the development of a regulatory framework for national detection strategy or nuclear security detection architecture, (ii) the roles of the competent authorities on nuclear security systems and measures, and (iii) international cooperation to improve effectiveness related to the detection function. The development of a regulatory framework could consider the scope and national priorities, threats assessment, and assessment of the selection of nuclear security detection architecture. Threat assessment should be conducted to determine several things such as the amount of nuclear material and radioactive sources, enemy characterization (attributes, abilities, and tactics that can be used), strategic targets and locations, and locations where nuclear material and radioactive sources going in and out.
roles of the competent authorities is based on the duties and functions of each competent authority as well as cooperation and coordination mechanism among competent authorities.

Keywords: nuclear security, national, regulation, detection, architecture, development

State
Indonesia

Gender
Male

**Primary author:** Mr YUWANA, Hermawan Puji (Nuclear Energy Regulatory Agency of Indonesia (BAPE- TEN))

**Presenter:** Mr YUWANA, Hermawan Puji (Nuclear Energy Regulatory Agency of Indonesia (BAPE- TEN))

**Track Classification:** CC: National nuclear security regulations
Commonization of Nuclear Security in Policing Malaysian Major Cities

Most police officers in Malaysia will frown upon mentioning of nuclear security in normal policing. This is because the phrase is not common to their police lingo even though it is attached to the word security. Some will say nuclear security is something related to what scientist do in lab, some will relate it to nuclear bomb, others will say this is an academic issue, some go to the extent that nuclear security is not related to Malaysia because we do not own nuclear bomb, some will even ask back what constitute nuclear security and some will shrug off the issue. These examples are not to undermine or underrate the Malaysian police. The police top brass is capable of understanding the issue of nuclear security, but they do not patrol the street on a daily basis. The one who is manning the streets, meeting the community, performing crime watch, and other crime prevention initiatives is the one who should be familiarized and empowered with the phrase of nuclear security and what does it means in a bigger threat context. These field officers including those routinely patrolling the city limits must be sensitized on the inclusion of nuclear security function in their daily tasking. Middle level managers and supervisors are the essential disseminator or propagator of nuclear security. In meeting room, during daily briefing or shift briefing, apart from normal crime prevention issues, suffice that managers and supervisors include nuclear security reminder as 5% of the briefing contents. Over time, nuclear security will slowly but surely be embedded in their hearts and minds. It takes simple mindful approach to propagate nuclear security. It must be structured and strategized to reach the targeted group. Before embarking into this program, of course, it is essential to get the buy in from top leadership of the police force. Without genuine leadership’s will, any good program will not survive the test of time. Sustainability is the key factor to a successful integration of nuclear security into day-to-day policing. To start with, forget about any instrumentation. Nuclear security should be introduced in simple plain language to commonize it among targeted officers. First group of targeted officers are those from the middle management and supervisors. Once they understand the subject matter, some forms of reading materials are given to them for self-reading to invoke questions they may have later on. For this purpose, a dedicated officer from the regulator will be introduced to them as resource person. No pressure, just a genuine leisure reading in their spare times. While the middle managers and supervisors absorbed new material in their daily job, the second targeted group will have some fun learning and understanding nuclear security program in an interactive classroom setting. It should be a half-day informative event with creative contents just to connect them with nuclear security. Instrumentation is only mention in passing so they can follow through later when detection equipment made available to them. For ready state deployment, focus is given to this existing work force but parallel to this a different classroom contents can be designed for new intake. Apart from standard police trainee modules, the new intake class will have a special 6-hour module including practical time to play around with the various detection instruments in various scenario settings. This will prepare them the basic understanding of nuclear security once they are deployed to various police formation throughout the country. It will work even without the instrument because awareness is more important than having an instrument but did nothing when it raise the alarm. To further commonize nuclear security, we must virtually detach it from any special force or special unit like CBRNE team so normal policeman will also feel responsible when confronted with nuclear security situation and will take immediate action while waiting for a backup team of specialist to arrive. Let nuclear security be a common thing among the police personnel starting from day one at the training centre with only a fraction of the training time.
Approach to training is important because with limited instruments, we are banking on high level of awareness. If the trainee can retain information about nuclear security after graduating from training centre, it is a good sign he will remember it throughout his career as a policeman or officer. Make nuclear security something light and easy, use a lot of visualization and association in teaching technique. For example, inviting iconic figure or personality to perform demo or do role play for the demo. The trainees will remember the iconic figure as mental image and relate it to nuclear security or to whatever contents that have been discussed. With this effort, in the long run, nuclear security can be part and parcel of daily policing.

State

Malaysia

Gender

Female

Primary author:  Ms ISHAK, Normah (Royal Malaysian Police)

Presenter:  Ms ISHAK, Normah (Royal Malaysian Police)

Track Classification:  CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
Indonesia has around 7,430 different types of radioactive sources from all categories (based on BAPETEN database, b@lis infara on 16 May 2019). Radioactive sources has been applied in industries, hospitals, and research centers and it is one of the most urgent and threatening dangers, as it can be used in dirty bomb and other malicious acts. Indonesian Nuclear Energy Regulatory Authority (BAPETEN) continuously enhances and improves the quality of its regulations with respect to security of radioactive sources. We have BAPETEN Chairman Regulation No. 6 Year 2015 on Security of Radioactive Sources, which is established and applied in facilities since 2015. Regulatory control must be implemented through development of regulations, reviews and assessment, authorization, inspection and enforcement.

The Analysis of this study is conducted to evaluate the process of formulating and composing BAPETEN Chairman Regulation No. 6 year 2015 on Security of Radioactive Sources. Important objects that are not covered by current regulation will be shared in this study and all the experiences and lessons learned we obtained from it will be explained clearly in this study with the hope that it can be useful for other countries in their regulatory development process.

The Process of formulating and composing the Regulation No. 6 year 2015 on Security of Radioactive Sources was started when the previous regulation needed to be revised in the need of implementing Nuclear Security Series (NSS) No. 11 (2009) and No. 9 (2008), since the previous regulation was composed based on IAEA TECDOC 1355 (2003). We were working in team, the members of which had clear understanding in relevant issues to be addressed in this regulation. We also accommodated stakeholder’s input in our regulation, and after the final draft was reviewed, we posted the final draft at BAPETEN website to receive input from stakeholders.

The experience we can share in this study is when we tried to regulate the storage facility of industrial gauges with high activities sources and well logging. We have enough resources but we still got confusing in regulating the facility and the storage within the facility (bunker). Finally we decide to regulate the industrial gauges with high activities sources and well logging in the category 3 (have to meet the security level 3 requirement) in accordance with NSS No. 11. However, for the bunker of industrial gauges and well logging sources (the storage facility) need to meet security level 2 requirement because of the aggregation of the source. This was not mention in the NSS No. 11, so we create this because of the condition in the facility.

The lesson learned we gather from this regulation development process is that we realized that some important objects are not covered by current regulation, such as the security level of the aggregation of radioactive sources during transport and facilities with radioactive sources that already decayed, didn’t go to a lower security level requirement, and the use of radioactive sources having A/D ratio did not match with the practice based, for example the radioisotope generators for radiopharmaceuticals production in PET scan facility at hospital, had low A/D ratio but it had to follow high security level requirement. This will be our homework for the next revision.

The development of regulations concerning safety, security and safeguards which included planning, drafting, discussion, legitimation, enactment, and dissemination was successfully finalized in 2015. We experienced difficult time in composing the regulation on the storage bunker within the facilities of industrial gauges with high activities sources and well logging, we also learned that some important objects are not covered by current regulation. Therefore we hope our experiences and lesson learn will be useful for other countries in their regulatory development process.
State
   Indonesia

Gender
   Female

Primary author: SAWIYAH, Sawiyah (BAPETEN)
Co-author: Mr RAHADHY, Soegeng (BAPETEN)
Presenter: SAWIYAH, Sawiyah (BAPETEN)

Track Classification: CC: National nuclear security regulations
Development of Nuclear Security Technologies for Response on Material Out of Regulatory Control Event and Nuclear Forensics Activities in Japan

A nuclear security event involving nuclear and other radioactive materials out of regulatory control (MORC) has potential severe consequence on public health, environments, economics and society. Therefore, each state has responsibility to develop national nuclear security measures including the response on any nuclear security events. Japan Atomic Energy Agency (JAEA) which is the national nuclear research institute, and National Research Institute of Police Science (NRIPS) which is an attached organization of national police agency in Japan, have been working on technology development for event scene activities and nuclear forensic activities to establish the capabilities for responding MORC related nuclear security event. These research institutes from different research fields have information exchange and have initiated a discussion for future cooperation for more effective implementation and improvement of the national capabilities and strengthening international nuclear security. In this paper, current status and future prospects on technology development in the two institute in Japan for contributing to the response capabilities for nuclear security event involving MORC.

In accordance with Japan’s national statement at the first Nuclear Security Summit, Integrated Support Center for Nuclear Nonproliferation and Nuclear Security (ISCN) was established in JAEA, and ISCN has initiated nuclear forensics technology development for contributing to the identification of origin and history of MORC. ISCN has established fundamental nuclear forensics analytical capabilities to characterize nuclear materials and prototype nuclear forensics library for interpretation of the analytical results. These technical capabilities have been validated through the joint research with the U.S. national laboratories and EC-JRC, and participation in exercises organized by ITWG. ISCN has also engaged in development of advanced technologies for more rapid and precise nuclear forensics analysis and shared the achievements for strengthened international nuclear forensics capabilities. Recently, ISCN has initiated the development of nuclear forensics technologies for post-dispersion event and innovative nuclear forensics technologies. The post-dispersion technology includes the supporting technology for detection and recovery of radioactive samples in event scene, and measurement and interpretation methodologies targeting post-dispersion samples. As the innovative technology, application of new technologies has been studied, such as machine-learning algorithm for nuclear forensics interpretation and autoradiography for supporting traditional forensics on contaminated evidence.

NRIPS conducts the research in forensic science and applies it in the examination and identification of evidence collected during police investigations. The physics section in NRIPS has developed the first responder equipment for nuclear detection and for sampling and categorization in nuclear forensics. In recent research, a radiological-threat scenario produced with Monte Carlo particle transmission simulation code and a survey system of radiological residue that performs real-time measurements of distributed sources in situ are studied in NRIPS. NRIPS also has developed a radiation detection simulator using smartphones and Wi-Fi beacons. This simulator helps the training for searching suspicious radiological sources and for screening of people for contamination. Additionally, the simulator using GPS on a smartphone is studied for control boundaries in nuclear security event involving MORC. This method can be used not only for countermeasures against radiological threat but also for training of nuclear disaster and radiation education.

State
Japan
Gender
Male

Primary authors: KIMURA, Yoshiki (Japan Atomic Energy Agency); TSUCHIYA, KENICHI (National Research Institute of Police Science); OKUBO, Ayako (Japan Atomic Energy Agency); TANABE, Kosuke (National Research Institute of Police Science); KAKUDA, Hidetoshi (National Research Institute of Police Science); AKIBA, Norimitsu (National Research Institute of Police Science); TOMIKAWA, HIROFUMI (Japan Atomic Energy Agency)

Presenter: KIMURA, Yoshiki (Japan Atomic Energy Agency)

Track Classification: MORC: Nuclear forensics
The need for computer security at nuclear facilities

In light of the growing threat of attacks on the IT of critical infrastructures, states need to take steps into protecting systems that are vital to the safety and security of such installations. Nuclear facilities are just of one the installations, that are of particular interest to groups that are looking into either disabling a countries power grid or to actually try and cause physical damage and thereby possibly causing the release of radioactive material.

The capabilities of hackers are increasing with time, as tools developed and used by state actors are getting available, therefore the security of the IT infrastructure needs to be continuously monitored. For Nuclear facilities, a rigorous system is needed, in which the IT used in the facility is analyzed and hardened against attacks. Most nuclear power plants will have been built at a time, when threats through attacks on IT systems were unlikely or even impossible. In time, these installations were upgraded with IT systems, which now need to be analyzed as to the potential risk they might pose were an attacker to be able to gain access to or even control of such system. This can be a complicated and involved process that may take years.

In this presentation we will highlight the approach taken in Germany and point out the advantages that come with that approach.

State

Germany

Gender

Male

Primary authors: Dr MERGEL, Edgar (BMU); ELSNER, Thomas (BMU)

Presenters: ELSNER, Thomas (BMU); KROEGER, Helge

Track Classification: CC: Information and computer security considerations for nuclear security
The intricate security culture issue: some considerations about the role of managers

This paper deals with the importance of a positive leadership for a well-fostered nuclear security culture in practice and the impact the behavior of managers can have to it. This goal of robust and positive security culture is not restricted to the classical security area but also indispensable for an effective cyber security culture as well. While it is easy to state and demand for appropriate management skills of managers, this question is quite intricate when it comes to the leadership behaviour and its impact to the security culture of the overall staff.

One problem may arise from the fact that the goals of the organization are maybe not 100% identical with the goals of its staff and the other problem is the definition of a good leadership itself as it remains somehow vague or dizzy what good leadership is based on. Fostering a robust positive security culture is not given by itself: it is based on a carefully chosen and balanced action by the managers who are in charge to act as leaders and be role models for the general staff. Whereas they are supposed to guarantee a tailor-fit management system for themselves and their coworkers, the role modelling function of managers should not be underestimated. Taking into account the IAEA Nuclear Security Series No. 7 "Nuclear Security Culture" (implementing guide, 2008) one can easily identify the characteristics of leadership behavior which are supposed to support a strong security culture of the overall staff, such as
(a) Expectations,
(b) Use of authority,
(c) Decision making,
(d) Management oversight,
(e) Involvement of staff,
(f) Effective communications,
(g) Improving performance and
(h) Motivation.

These characteristics should however be breaking down and translated to a more handy or practical format. Besides they are supposed to be more thought provoking than prescriptive because an effective leadership of the managers cannot be realized by simply parroting high but formal demands for the so-called appropriate behaviour of the managers. What does that mean in practice for the managers? They are indeed in charge of questioning their own daily behavior, e.g. by asking themselves e.g. the following questions:

- How do I guarantee to be regularly and often approachable for my staff?
- How do I take responsibility for the needs of my staff?
- How can I ensure to visibly act as role model when it comes to security related issues (and not claiming "special rights" and exceptions for myself)?
- What can I do to clearly and regularly communicate the security goals of our company to the staff?
- How do I contribute to improve the motivation of the staff?
- How do I make decisions and do I properly explain them to the staff?
- How do I use authority and if so, everytime if necessary and or just limited to sanction the staff?
- How can I clearly communicate the "red line" problem (the absolute "no-go" for our company when it comes to security related behaviour) and the obligatory consequences if crossing or violating this line?
• Do I regularly perform walkthroughs, make them visible for the staff and document them in a careful and respectful manner?
• How do I motivate and actively support the (self-)assessment of our own security culture?
• How do I contribute to implement the resulting action plan and monitor its progress?

Managers are therefore obliged and should feel responsibility to frequently reflect their own behaviour in regard to an overall strong security culture and optimize their own behaviour whenever necessary. Complacent or even ignorant managers should not expect a better security-oriented behaviour from their staff than from themselves. Only a positive and well-fostered security culture will contribute to an effective security regime.

State
Germany

Gender
Male

Primary author: Mr SPEICHER, Carsten (Ministry of the Environment, Climate Protection and the Energy Sector, Baden-Württemberg)

Presenter: Mr SPEICHER, Carsten (Ministry of the Environment, Climate Protection and the Energy Sector, Baden-Württemberg)

Track Classification: CC: Nuclear security culture in practice with a focus on sustainability
HUMAN FACTORS EVALUATION IN OPERATORS WITH ATTENTION TO INSIDER THREAT DETECTION

AUTORS: Antonio C.A. Vaz; Vinicius F. Borges and Frederico A.Genezini

ABSTRACT

A key concept in nuclear reactor operation is that nuclear security is the result of interactions between human, technological and organizational factors. Nuclear Standards Regulatory understands how human factors from psychological, physiological, behavioral and emotional origin can affect the reactor security. For that reason, reactor operators are submitted to rigorous evaluations every year. When conducting case studies during these sixty years of IEA-R1 reactor operation, three of them related to security illustrate the concern about this issue: Case 1- Contract workers tried to steal lead used in the shielding of water treatment system. Case 2- Operator suffered stress in traffic in his going to the reactor facility; when performing test in the emergency cooling system for reactor start up, he didn’t close a valve completely; changing the pool water technical quality causing a week delay in the reactor operation. Case 3- During fueling the reactor core, operator realized that the fuel element assembly was inverted. In the investigation verified that assembler man’s father had passed away three weeks before the fuel element assembling. There was sabotage speculation by the manager. This multidisciplinary work aims to include human factors of psychological and behavioral origin as preventive and protective measures of the reactor physical protection system, focusing insider threat detection. Technologies associated with neuroscience and psychological assessments such as: Face Reader, Analogue Visual Mood Scale and Back Depression Inventory; allows the operator evaluation in the facility. However, problems like described in the case studies should be elucidated. Insider threat is one of the biggest concerns of globalized society. Through the human and technology interaction, several research studies have been carried out to ensure that preventive and protective measures are taken to minimize, mitigate and mainly prevent insider actions. Understanding the role of nuclear security in keeping its facilities protected, this research proposes to study interface between man and technology aims the insider threats detection. So the technology will allow the possibility of detection to be made in preventive and mainly protective way. Through the philosophy of defense in depth technology will prevent a possible insider to access a vital area, detecting an insider before the start of malicious act. For example, technology would detect the German Wings-FLIGHT 9225 pilot wouldn’t have the psychological conditions to conduct the airplane that day. While advanced data analytics techniques can help organizations objectively evaluate insider behaviors and enhance their security posture, they are not enough. Organizations should combine the use of technology with well-defined policies, consistent communication and training, and routine due diligence. Standardizing on boarding, background screening and employee separation procedures will also offer opportunities for mitigating harmful activities.

This work will be presented in Poster Session.

State

Brazil

Gender
Male

**Primary author:** Mr VAZ, ANTONIO (Brazilian Nuclear Commission-IPEN/CNEN-SP/BRAZIL)

**Presenter:** Mr VAZ, ANTONIO (Brazilian Nuclear Commission-IPEN/CNEN-SP/BRAZIL)

**Track Classification:** PP: Insider threats
Computer and information Security (Cyber Security) Training and Awareness Program for Nuclear Facility

The risk to nuclear facilities from cyber attacks is increasingly perceived as a growing, real problem due to entrance of new adversaries (e.g. ISIS) and the advancement of capabilities of existing adversaries such as criminal organizations and nation states. Recent sophisticated attacks have targeted instrumentation and control (I&C) systems having significant potential consequences for security and safety. This increasing risk has resulted in the recognition of cyber security as an essential element of the overall security framework of nuclear facilities and as such is a pressing priority for facility operators and national regulators.

A critical computer security measure is cyber security awareness and specialist training for all personnel. Provision of training is an administrative control measure, needs to be required by Computer Security Programme (CSP) and implemented in the organization’s training programme. When considering the requirements for training, it is important to have a risk informed approach. This begins with the assignment of personnel to roles and responsibilities to address risk associated with cyber security. These personnel require specialist training consistent with the risk associated with deficient or ineffective performance of their roles and duties.

However, the training programme must consider all personnel to provide an effective first layer or defence. As per the Verizon 2019 Data Breach Investigations Report [1], 94% of malware was delivered via email, and Social Engineering attacks were involved in 33% of attacks leading to breaches. Therefore, a training programme providing awareness training on cyber security is essential to enhance cyber security culture for all facility personnel.

This paper will provide evidence the importance and urgency of cyber security awareness and training is underestimated at present, and also provide recommendations on the types, trainees, contents, and development strategies of cyber security awareness and training programs to guide nuclear facility operators to deliver effective cyber security training.

State
Ghana

Gender
Male

Primary authors:  AGBEMAVA, Nelson Kodzotse (Nuclear Regulatory Authority- Ghana); ROWLAND, Michael (Practical Reason Incorporated); GYEKYE, Prince Kwabena (Nuclear Regulatory Authority)

Presenter:  AGBEMAVA, Nelson Kodzotse (Nuclear Regulatory Authority- Ghana)

Track Classification:  CC: Nuclear security culture in practice with a focus on sustainability
On demand production of a Pa-233 tracer

Uranium radiochronometry is of great interest to the nuclear forensics community [1–3]. The $^{235}$U/$^{231}$Pa isotope pair can be used to calculate the separation age of samples containing enriched $^{235}$U; a comparison with another radiochronometric pair, $^{234}$U/$^{230}$Th, can provide additional information about the processing history of the material. Accurate dating using the $^{235}$U/$^{231}$Pa nuclear chronometer typically requires access to the short-lived radiotracer $^{233}$Pa ($t_{1/2} = 26.98(2)$ d) [4], which is used to quantify the longlived $^{231}$Pa ($t_{1/2} = 32.8$ ky) by methods such as isotope dilution mass spectrometry [5, 6]. The short lived $^{233}$Pa is ideal for decay counting primary standardization using coincidence counting and liquid scintillation counting (LSC) methods.

At the present time, access to $^{233}$Pa is limited to the handful of laboratories around the world that possess significant quantities of $^{237}$Np ($t_{1/2} = 2.14$ My). As a decay product of $^{237}$Np, $^{233}$Pa forms continuously in situ, and can be isolated by complex chemical processing of these neptunium sources [5]. However, due to the long half-life of $^{237}$Np, significant quantities of $^{233}$Pa can only be generated after an interval of months from the previous source reprocessing, limiting its access upon immediate requisition. If the $^{235}$U/$^{231}$Pa dating method is to be applied as a forensic tool in emergency response scenarios, access to $^{233}$Pa must be improved significantly.

The deliberate generation of $^{233}$Pa by bombarding natural thorium oxide with thermal neutrons was first reported more than 60 years ago [7]; but to our knowledge, this production route is not in use today. Although the reported post-irradiation processing is not appropriate for routine production due to the complex, multi-step chemical treatments and use of hazardous reagents including fluorine and hydrofluoric acid, the production physics of this process is near-ideal. Natural thorium is monoisoisopic (100% $^{232}$Th), and thus the sole product of its thermal neutron activation is the short-lived radioisotope $^{233}$Th ($t_{1/2} = 22$ min), which undergoes beta decay to the desired $^{233}$Pa. The moderate cross-section for the $^{232}$Th(n, $\gamma$)$^{233}$Th nuclear transformation ($\sigma = 7.4$ b) indicates that arbitrary (MBq) quantities of $^{233}$Pa can be generated using this production route even in low- and medium-flux nuclear research reactors. A re-investigation of the separation of $^{233}$Pa from neutron irradiated thorium to identify a methodology that is simple, rapid, and reproducible is therefore in order. The ideal approach would also avoid the use of reagents that require special handling, such as HF-assisted separations described elsewhere [8–10].

As one of the world’s leading producers and processors of uranium, Canada is interested in expanding its nuclear forensics capabilities for characterizing samples that are found outside of regulatory control. Towards this goal, the objectives of this work were two-fold: first, to investigate the feasibility of “on-demand” production of $^{233}$Pa from thorium at the McMaster Nuclear Reactor, the nation’s most powerful research reactor; and second, to conduct standardization measurements at the National Research Council of Canada. The resulting certified reference materials could be used to calibrate secondary radioisotope quantification instrumentation.

References:
5. Eppich GR, Williams RW, Gaffney AM, Schorzman KC (2013) $^{235}$U–$^{231}$Pa age dating of ura-

State

Canada

Gender

Male

Primary authors: Dr GALEA, Raphael (National Research Council of Canada); Ms NAPERSTKOW, Zoya (McMaster University); Dr ARMSTRONG, Andrea (McMaster University)

Presenter: Dr GALEA, Raphael (National Research Council of Canada)

Track Classification: MORC: Nuclear forensics
Radioactive materials play an important role in commercial, medical, and research facilities across the world. However, the benefits of these sources must be balanced with sufficient security to prevent radiological materials from falling into the wrong hands. In its efforts to prevent high-activity radiological materials from being used in acts of terrorism, the Department of Energy’s (DOE) National Nuclear Security Administration (NNSA) Office of Radiological Security (ORS) helps reduce the global reliance on high-activity radioactive sources by leading efforts to support the adoption and development of non-radioisotopic alternative technologies. ORS engages in efforts internationally to exchange technology information with users of cesium-137 based irradiators who are interested in converting to viable non-radioisotopic alternatives and understand and reduce obstacles preventing the transition to an alternative technology.

As the maturation of technology has led to the availability of non-radioisotopic alternative technologies, many countries are exploring the transition from cesium-based blood irradiators to x-ray based blood irradiators. Today, there are six x-ray irradiator models that have been approved for use in this application in the U.S. and European Union, facilitating this transition.

The first such alternative technology project under the ORS program has been replacement of a cesium chloride blood irradiator at the Espanola Hospital in Montevideo, Uruguay. In this case, both because it was a project implemented outside the U. S. and because of circumstances unique to Uruguay, implementation of the project presented a unique set of challenges. Those challenges, and how the site and the relevant Uruguayan regulatory agencies addressed those challenges, have provided policymakers, regulators and site operators with lessons learned and tools to assist in implementation of future international alternative technology projects.

These tools have come about because of the need to address a range of issues and requirements, including:

1) The participation and agreement of the relevant in-country regulatory agencies and the need to satisfy regulatory requirements for licensing and operation of a new medical device.

2) The need to work with the site facilities personnel, in addition to the medical personnel, to establish clear requirements for infrastructure modifications required to install the x-ray device, including electrical and cooling requirements;

3) The proper pathway and paperwork necessary to have the x-ray device clear Customs once it arrives in-country;

4) Ensuring the availability of timely local technical support in case problems should arise with the replacement device either before or following delivery and for follow-on preventive maintenance. In some cases, this may involve factory authorized training for a local or regional service provider; and

5) Confirmation of a safe and secure disposition pathway for the existing cesium or cobalt unit, which would include having licensed companies be able to remove the device inside or outside the country, remove the sources safely and securely and dispose of them according to relevant regulations.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy’s National Nuclear Security Administration under contract DE-NA0003525. SAND2019-XXXX A
State

United States

Gender

Female

Primary authors: Mr LIEBERMAN, Jodi; Dr CABRAL, Walter (MIEM-ARNR); FALLER, Blanca

Presenter: Mr LIEBERMAN, Jodi

Session Classification: Innovative technologies to reduce nuclear security risks and improve cost effectiveness, where feasible

Track Classification: CC: Innovative technologies to reduce nuclear security risks and improve cost effectiveness, where feasible
Implementing blockchain technologies in NMAC system

Emerging technologies have focused on blockchain technology. Its growing use in the industry motivates the review of possible applications in the nuclear production. For instance, the French Atomic Energy Commission (CEA) developing a blockchain solution to increase trust in the food and Rosatom (Russia) invest in R&D on blockchain to safeguard military assets.

On the other hand, the IAEA has developed a general guide on the use of a nuclear material accounting and control (NMAC) system in support of nuclear safety at the facility level. The objective of these control measures is to maintain the continuity of nuclear knowledge in order to detect unauthorized waste, involving people with access to sensitive information. The control of nuclear material is carried out during the production, processing, use, storage and, movement of the same. The contribution of this work is the implementation of the NMAC system using blockchain. In this sense, blockchain is a technology that could be used to archive the completed control and accounting to provide transparency in each step of NMAC. Also, it is a perfect tool to avoid proliferation issues.

Blockchain constructs a chronological chain of blocks, hence the name “block-chain”. Each block is an immutable information unit. Also, Blockchain consists of timestamping of transactions, Peer-to-Peer networks, cryptography, and shared computational power.

Each nuclear material custodian is responsible for one-material-balance area. An area in a nuclear facility is a location where the quantity of nuclear material in each movement can be determinate. That is why the different material balance areas are the basis for NMAC system for all nuclear material in the facility. The quantity and attractiveness of the nuclear material determine the control type applied for its protection.

The guide about NMAC, advises that a registry documenting the implementation of all control measures of nuclear materials must be kept. These records must include a brief description of each nuclear material control activity, the signatures of the personnel who carry out the activities and the dates in which they were carried out. The registry must be kept secured and must be available to those who require access to them in the event of an irregularity or when an audit of the nuclear material control system is conducted.

Nuclear material control measures include, but are not limited to, control of access, material containment, tamper indicating devices (TIDs), nuclear material surveillance, monitoring of nuclear material items, monitoring of nuclear material during processing, and physical inventory taking.

The use of TIDs with a unique identification feature provides a level of confidence that the item protected by it has not been opened. During nuclear material movements, TIDs may be applied to nuclear material containers, shipping containers, and the transport vehicle cargo compartment, to provide for both the shipping and the receiving entity that the container and compartment integrity of the containment has not been violated. The TIDs are commercially available as, for example, electronic radio frequency tags. The limitation is that a TID could be replaced, removed, reapplied, or altered without leaving any indications of tampering. As a consequence, blockchain technology is presented as an unparalleled solution to ensure the registration of each activity carried out on a unit of nuclear material.

Operations involving nuclear material should be authorized and planned appropriately. There should be clear communication and sharing of information, among: management, NMAC, physical protection, safeguards, safety, and operations personnel regarding operations involving nuclear material (particularly with the confidentiality of sensitive information). Blockchain technology
helps store and verify information in a decentralized way, using cryptographic techniques, where each transactional block is timestamped.

Accordingly, blockchain technology is a perfect digital solution to carry out the control of nuclear material. The business network should be composed of: each material-balance area custodian, the facility manager, and the nuclear authority to track the movement of nuclear-material. Each participant is able to access and work upon information about nuclear material store in a block. It could be possible to specify which is the nuclear element involved, its category, what kind of physical control should be exercised, the nuclear material custodian, the balance area, TID code, in each block of the chain. However, digital signatures could be used; however the block hash should be enough. The implementation of this scenario is simulated using IBM Hyperledger Framework.

As a brief conclusion of this work, blockchain technology promises an NMAC system efficient and transparent. Respectly to information security, being a distributed database, availability is guaranteed. Blockchain helps solve the vulnerabilities introduced with the use of TIDs since every activity carried out on a unit of nuclear material is recorded in a timely manner.

State
Argentina

Gender
Female

Primary author: Ms VENTURINI, Veronica Mariana (Argentinian Atomic Energy Agency)
Presenter: Ms VENTURINI, Veronica Mariana (Argentinian Atomic Energy Agency)

Track Classification: PP: Nuclear material accounting and control
Common Criteria for Nuclear Cyber Security

The nuclear industry is just one of many industry verticals (e.g. automotive, medical, oil & gas etc.) grappling with the challenge of addressing cyber risk in the supply chain. The Common Criteria (ISO/IEC 15408) is the only well established and internationally recognized standard for the security evaluation of IT products – a vital part of the supply chain. Uniquely, the Common Criteria provides a flexible but structured framework that can be customized and adopted for a variety of industry vertical use cases, threat models and assurance levels. Coupled with the standard itself, there exists a world-wide network of Common Criteria schemes and labs that can be leveraged by the nuclear industry.

In his presentation, Mr. Turner will provide the following information to delegates:

- Basic introduction to Common Criteria
- Relationship between Common Criteria and EU Cyber Act (as this will be of interest to many of the delegates)
- Using Protection Profiles to specify security requirements
- Examples of how Technical Communities collaborate to create Protection Profiles
- Examples of how test automation is being leveraged to speed up Common Criteria evaluations
- Applying Protection Profiles and Technical Communities collaboration in the Nuclear context (a concrete example of how CC can work in the Nuclear context)
- Regulatory examples and recommendations

The three key points that Mr. Turner wishes to leave with the delegates are:

1. Don’t re-invent the wheel. The Common Criteria (ISO/IEC 15408) is the only well established and internationally recognized standard for IT product security evaluation – and it is improving all the time. There is tremendous value in the world-wide network of schemes and accredited labs that can be leveraged for your industry. Uniquely, the Common Criteria provides a flexible but structured framework that can be customized and adopted for a variety of industry vertical use cases, threat models and assurance levels.

2. Industry collaboration is critical. The Common Criteria is like a tool box – one must know which tools to use. To get real value from Common Criteria, industry participants must collaborate to:
   a. Create a market demand (or regulator requirement) for Common Criteria – vendors will not go to the trouble of certification if there is no demand.
   b. Create tailored requirements to address the specific industry needs – leverage the Common Criteria User Forum to establish Technical Communities that are focused on sharing threat intelligence and specifying security requirements (both functional and across the product life-cycle) for technologies that are critical to your industry – i.e. via Protection Profiles.

3. Automation is here. It is only through industry adoption of test automation that the Common Criteria process will scale and be able to adequately address the current shortcomings that prevent the wider adoption of the standard for other verticals – namely time, cost and demonstrable reduction of risk.

State
Canada

Gender
Male
Primary author:  Mr TURNER, Lachlan
Presenter:  Mr TURNER, Lachlan

Track Classification:  CC: Information and computer security considerations for nuclear security
Indirect Impact of Infrastructure Development Programs on Security in Transport of Radioactive Material in Indonesia

Indonesia is catching up with infrastructure development in recent years. Based on the World Economic Forum 2013 data, Indonesia’s infrastructure is ranked 64 out of 148 countries in the world. Meanwhile, Indonesia’s ranking in ASEAN is ranked 5th after Vietnam. The main purpose of this development is to improve the economy and business in Indonesia. However some aspects should be considered as they might contribute in direct impact to the development, one of which is security in transport of radioactive material.

The transport of radioactive material is usually an interim phase between production, use, storage, and disposal of the material. The modes of transport should be taken into account when designing the transport security system. The total time that radioactive material is in transport, the number of intermodal transfers and the waiting times associated with the intermodal transfer are kept to the minimum necessary.

From 2014 to 2018, Indonesia has built along 3,432 kilometers roads and 947 kilometers of toll roads. The toll roads of concern are the Trans Sumatra toll road and the Trans Java toll road. Bakauheni-Palembang toll road in Sumatra is expected to have a significant impact on security in transport of radioactive material. The toll road is divided into 2 sections, Bakauheni-Terbanggi Besar (140km) which has been operating since March 2019 and Terbanggi Besar-Palembang (220km) which is estimated to be fully operational by the end of 2019. This toll road becomes important for security in transport of radioactive material because South Sumatra is one of the largest oil producers in Indonesia, so that industrial radiography activities are also quite high. Companies providing industrial radiography services from Java island usually use land transportation after crossing the Sunda Strait that passes through Lampung to reach the location of the oil industry in South Sumatra. Before the construction of the toll road, the road across Sumatra had a high crime rate of theft with violence, especially in Lampung. With the existence of the Trans Sumatra toll road, travel time can be reduced and toll road security is also maintained. Therefore it can reduce the threat of security in transport of radioactive material, especially for industrial radiography in South Sumatra and Lampung.

The Trans Java Toll Road also has an important impact on the security in transport of radioactive material. The toll road has connected Jakarta and Surabaya, the 2 largest cities in Indonesia, with a the length of 760 km. The travel time for Jakarta-Surabaya will be significantly reduced, from 20 hours passing the national road, to less than 15 hours passing the toll road. Therefore the travel time of transportation of radioactive material in the Java Island can be reduced, which also reduces the threat of security in transport of radioactive material.

Indonesia also develops infrastructure for information and communication connectivity. The Palapa Ring, which involves an undersea fiber-optic cable network that stretches across 13,000 kilometers as well as an onshore network of nearly 22,000 kilometers, will provide fast broadband Internet to Indonesian people in both the urban and rural areas across the country. Once completed, all Indonesian districts (Kabupaten) are connected through fiber-optic communication. The development of connectivity infrastructure is dedicated to facilitating the mobility of people working and doing business, increasing the distribution of goods and services, and increasing people’s productivity and competitiveness in the international market. But this infrastructure can also support the security in transport of radioactive material. For packages of radioactive material with contents meeting or exceeding the radioactivity threshold for the enhanced security level tracking
measure should be applied. Tracking methods or devices may be used to monitor the movement of conveyances containing radioactive material. A simple tracking system will be able to track when a shipment has departed, whether the mode of transport has changed and if the material has been placed in interim storage or the consignment has been received. This information about status changes should be readily available to the appropriate parties. The tracking system, in conjunction with a communications system and response procedures, will allow the operator and the competent authority to react in a timely manner to a malicious act, including theft of radioactive material.

In addition to the above benefits, there are also challenges for the security in transport of radioactive material due to the increased infrastructure development. From 2014 to 2018, 19 new ports have been built and existing ports revitalized. The government also plans to make seven ports in Indonesia an international hub to compete with Singapore. The need for Radiation Portal Monitor (RPM) is increased to ensure the security in transport of radioactive material. At present, there are only 6 units of RPM installed in Indonesia in 6 locations, Tanjung Priok, Batam, Bitung, Makassar, Belawan and Semarang ports.

**State**

Indonesia

**Gender**

Male

**Primary author:** DWIPAYANA, Chrisantus Aristo Wirawan (BAPETEN)

**Presenter:** DWIPAYANA, Chrisantus Aristo Wirawan (BAPETEN)

**Track Classification:** PP: Transport of nuclear and other radioactive material: practices, challenges and regulatory issues
Pilot of the International Atomic Energy Agency’s Advanced, Practitioner-Level Training Course on Preventive and Protective Measures Against Insider Threats

The “Joint Statement on Mitigating Insider Threats” circulated by the International Atomic Energy Agency (IAEA) as Information Circular (INFCIRC) 908 emphasizes the elevated threat to nuclear and radioactive materials and facilities posed by insiders. To support States in mitigating this threat, INFCIRC 908 includes a commitment by the subscribers to support the IAEA in developing and implementing an advanced, practitioner-level training course on preventive and protective measures against insider threats. Subscriber States have fulfilled this commitment through developing the course materials and piloting the course 15-19 July 2019 at Sandia National Laboratories in Albuquerque, New Mexico, United States of America. This course reflects a strong international collaboration with course development and subject matter expert contributions from nine Member States and Interpol.

The course goals include that participants will leave the course with the following: (1) an outline of key elements of an insider threat mitigation program to take home and use as a roadmap for improvements, (2) international examples of how these elements can be successfully implemented in a variety of nuclear facility types, (3) new knowledge and skills to assist in assessing the effectiveness of their own programs, (4) knowledge of current research and forward leaning topics related to insider threats, and (5) an understanding of the importance of validating measures and procedures as defined on paper with real implementation and operational information.

This advanced course builds on the existing IAEA Nuclear Security Series No. 8 (Implementing Guide titled Preventive and Protective Measures against Insider Threats), e-learning, and classroom-based training courses by incorporating hands-on activities in a mock facility, allowing course participants to apply skills in a realistic environment. The opportunity to use the mock facility enables this course to address the course goal that participants appreciate the importance of understanding not only how insider threat mitigation measures and procedures are designed and documented, but also how they are truly implemented in a specific facility. Mock facility activities highlight common implementation issues, as identified by the international team of subject matter experts developing the course.

Course lectures and panel discussions allow current practitioners to present their experience with key areas of insider threat mitigation, including threat characterization and assessment, personnel characterization and vetting, computer security measures to prevent insider threats, and prescriptive, performance-based, and combined approaches to system evaluation for insider threats. These lectures and panel discussions provide participants with examples of currently implemented good practices at a variety of nuclear facilities around the world that they could potentially apply to their own facilities to improve their insider mitigation programs.

In addition to lectures and panels from international practitioners, the course includes presentations on current research areas and forward-leaning topics addressing significant challenges to insider threat mitigation, including coercion, collusion, and supply chain impacts.

This paper will describe the course, outcomes of the course, and opportunities to extend the reach of this course in the future.

State

United States
Gender

Female

Primary author: Dr ASKIN, Amanda (Lawrence Livermore National Laboratory)

Co-authors: Ms BROWNELL, Lorilee (U.S. Department of Energy, National Nuclear Security Administration); Mr LARSEN, Robert (International Atomic Energy Agency)

Presenter: Dr ASKIN, Amanda (Lawrence Livermore National Laboratory)

Track Classification: PP: Insider threats
Organizational coordination in Indonesia for response to nuclear security events

Indonesia is the largest archipelago state in the world, approximately two thirds of which is water. In the perspective of radioactive sources utilization, especially on security aspect with that large territory and with many different cultures and local rules, the Indonesian government should have the right strategy to implement a security requirement that is set on Government Regulation and BAPETEN Chairman Regulation (BCR) regarding the utilization of radioactive sources on different areas (islands) in Indonesia. For radioactive mobile sources movement, transportation will be conducted mainly through the sea or river and land, making the risk for radioactive mobile sources from the security perspective is high. The utilization of radioactive sources in many areas in Indonesia also becoming high risk from the security perspective when it is in remote area.

Under Indonesia regulation, every operator of radioactive sources utilization should meet the security requirements to install, operate and maintain security system in order to detect and delay attempts to steal or sabotage a source. In dealing with security events such as stealing and sabotage of radioactive sources, operator of radioactive sources generally relies on external entities, such as local or national police or local government, national guard force, or some related organizations to respond to these security events. The challenges of faced with the security events are more difficult on Indonesia territorial because Indonesia has not only areas with established infrastructure and communication system but also areas with limited infrastructure and communication system. Therefore, the role of coordination between stakeholders regarding security system is very important.

BAPETEN as the Indonesian nuclear regulatory body has the role of establishing for setting requirements for security of radioactive source in facilities. One of the important requirements is that the operator should provide response function. The response function consists of providing response equipment and emergency response plan. This response function is stated in BCR No. 6 Year 2015. For To assist the operator in implementing response function, BAPETEN should make arrangements for achieving effective interagency response coordination among the stakeholders on the radioactive sources security aspect. Up to now, the International Atomic Energy Agency (IAEA) guidance on specific recommendations on how to achieve interagency response coordination has not yet developed.

Pertaining with the implementation of the above mentioned BCR, Indonesia, in this case BAPETEN, has made efforts to improve coordination by taking several steps, such as:
1. Identifying stakeholders along with their national duties and functions;
2. Providing education to stakeholders, especially law enforcement officers;
3. Collaborating and socializing with the local government;
4. Making cooperation agreements with stakeholders at the national level; and
5. Performing exercises to respond to nuclear security event based on the procedure at the facility.

For enhancing effectiveness coordination among stakeholders related to the response to security events, BAPETEN issued the BCR No.1 Year 2015 on Management of Emergency Response. This regulation states that Indonesia must establish an emergency response organization, establish procedures related to the response of nuclear security events and conduct training related to nuclear security events. At present, emergency response organizations in Indonesia also serves as response to organizations related to nuclear security events. This paper will highlight several efforts that have been taken by the Indonesian Government regarding coordination between stakeholders to respond to nuclear security incidents.
State

Indonesia

Gender

Female

Primary author: HAYANI, anet (BAPETEN)

Presenter: HAYANI, anet (BAPETEN)

Track Classification: MORC: Coordinated response to nuclear security events
The importance of Industry compliance to Ensure Nuclear Security and Growth in the Changing Times

Strategic Trade Control (STC) is one of the very strong pillars of Nuclear Security. Robust STC is an effective way to serve either as a deterrent and/or detection and delay the efforts of the proliferators to acquire WMD items or related technologies. An effective nuclear security must be a combined effort to balance the initiatives taken at international and state level [1-6]. There are multilateral controls regimes: NSG, WA, AG and MTCR whose main aim is to promote the non-proliferation and implement effective control mechanisms to ensure that legitimate trade in the strategic goods, dual-use goods, services and technology continues to grow, but to control the illegitimate trade to eliminate any possibility of such items falling in the hands of terrorist and other non-state actors with malicious intentions. The purpose of STC is not to deny the transfer of every conventional or nuclear weapon-related commodity or technology, but to ascertain that the ultimate end use is not for non-peaceful purposes. The two very important pillars for an effective STC is International Initiatives and State Regulation. An industrial compliance system (ICS) is a new concept which is now being introduced to improve the efficiency of export control licensing [7]. ICS is a system of checks and control within the company in order to ensure compliance with national regulations and policies and states may be encouraged for taking up for implementation of the same. The present paper highlights how an Industrial Compliance System (ICS) can be developed with combined effort of government and Industry.

For developing ICS in any state, government and Industry have distinct responsibilities for mutual reinforcing each other:

i) The Role of the government is to in develop policies and mechanisms to regulate and control trade with deterrence to proliferation efforts;

ii) The role of the Industry is to develop internal compliance systems to ensure strict adherence to governments’ policy and regulation;

iii) The need for Industry and governments to understand their responsibilities and work together with mutual coordination.

Development of ICS by Industry:

Robust STC in any state depends on the Industry awareness of their role to mitigate risks and enhance nuclear security. Effective STC is evolved on an interlocking set of national and international legislation, regulations, and agreements. The state legislations provide the basis to have a transparent and standardized national licensing system and to maintain competent technical evaluation of proposed transfers of nuclear-related materials, equipment, and technologies. Government should undertake outreach activities to industry to spread awareness about regulations and risk associated with the trade of nuclear related commodities. This help the Industry to develop the ICS. An effective ICS of an industry should ensure regulations as enacted by the government including export policies, control list and licensing procedure. The ICS of any industry should have standardized procedures to check credentials of the end user with whom they are doing business, stated end use, chain of transmission of items from foreign buyers, consignee to the ultimate end user, mode of financial transactions, capabilities of the recipient party, previous record of business with the end user etc. An industry is also responsible for training all its staff involved in trade of strategic items or technologies and must keep a complete documentation of all the trade related matters. An ICS prevent these Industry of doing business with unauthorized/shell companies which may prove to be a threat to global nuclear security.

The technical evaluations of export applications take into account the credibility of the end user and end use, assessed risk of diversion to rouge elements, capabilities of the recipient state, nuclear security measures instituted by the recipient state, applicability of the multilateral control regimes and other international obligations/agreements in the recipient state. The technical evaluation become very effective if industry has done the ground work as per the ICS. The government should make efforts to publish documents for procedures containing information for export/import licensing and is easily accessible to the industry. In addition, efforts should
be made to make hassle free communication between them and Industries regarding clarification or queries on any trade of nuclear related commodities and technology. When any legislation is introduced or amended in relation to STC, views from related industry associations should be taken into account. A close network between Government and Industry and understanding each other’s objective is a way to strengthen nuclear security. All these measures facilitate industries to develop mechanisms and follow ‘best practices’ for trade of nuclear related commodities.

References:
2. Code of Conduct on the Safety and Security of Radioactive Sources, IAEA.
3. INFCIRC/225/Rev.5: IAEA Recommendations.

State
India

Gender
Female

Primary authors: Mrs SHARMA, Garima (Scientific Officer); Mr PADMAKUMAR, S (Scientific Officer); Mr KUMAR, Ranajit (Scientific Officer)

Presenter: Mrs SHARMA, Garima (Scientific Officer)

Track Classification: CC: Contribution of industry to nuclear security
Supporting the Development of Technical Reachback for Nuclear Security Detection Architectures

Since 2017, the European Commission’s Joint Research Centre hosted two activities under the auspices of the Global Initiative to Combat Nuclear Terrorism (GICNT) that have addressed the topic of building or enhancing reachback support as part of national nuclear security detection architectures (NSDA). These workshops built upon the success of previous GICNT exercises that highlighted that nuclear detection requires a whole-of-government approach that incorporates technical and non-technical detection capabilities, including the integration of law enforcement and technical and scientific communities that support the detection mission.

The proposed presentation would highlight the outcomes from the March 2017 “Magic Maggiore” Technical Reachback Workshop and the February 2019 “Cunning Karl” Reachback Support Workshop. Some key elements of the envisioned presentation are included below.

- Summary of key findings from “Magic Maggiore” including common challenges and corresponding best practices
- Summary of key findings from “Cunning Karl” including an agreed upon definition of the term “reachback support” and a core list of capabilities for countries looking to develop reachback support as part of their national NSDA.
- Suggestions for how to utilize the outcomes from both workshops to support IAEA work in related areas.

“Magic Maggiore”

The “Magic Maggiore” Technical Reachback Workshop brought together a group of 60 technical, scientific, and operational experts to help raise awareness and build commitment towards technical reachback and to share best practices for addressing key challenges.

Outcomes from this event include best practices related to the following areas:

1. The role of technical support to nuclear security detection architectures
2. The role of threat assessments in informing the development of technical reachback
3. The role of information exchange between stakeholders
4. The need for concept of operations (CONOP) and standard operating procedures (SOP) for alarm adjudication
5. The role of technical and scientific experts in identifying equipment and instruments
6. The need for a common lexicon between stakeholders

“Cunning Karl”

The “Cunning Karl” Nuclear Detection Reachback Support Workshop built on the outcomes of “Magic Maggiore” by exploring strategies for countries looking to integrate reachback capabilities into their national NSDAs. Participants also worked together to define ‘reachback support’ in order to help build a common understanding and framework for future discussions.

Outcomes from this event include:

- A definition of “reachback” as an offsite entity that provides advisory and coordination support for operational, technical, analytical, and/or scientific matters.
- A list of core capabilities that would be essential for countries establishing or maintaining a national radiological and nuclear reachback support program or network. The list of core capabilities include:
  - Threat and risk assessment – to inform the level and scale of reachback support required
Legal frameworks – serve as the foundation for a country’s national nuclear security detection architecture (NSDA) and national response plan (NRP) and can prescribe the integral reachback support they contain

- Standard operating procedures (SOPs) – identify competent national and international authorities and coordination mechanisms between stakeholders, and describe related roles and responsibilities
- Communication plans – facilitate implementation of SOPs and should include secure and reliable national communication plans between front line officers (FLOs) and scientific experts and with relevant international stakeholders.
- Measurement capability – utilize radiological and nuclear detection equipment to detect the presence of radioactive material. A spectroscopic measurement device should be used during secondary measurements.
- Assessment capability – an entity, such as regulatory agency, university, or scientific institute, that has the ability to support detection operations by interpreting the cause of instrument alarms.
- Coordination role – consistent with SOPs and communication plans, coordinates further scientific support to FLOs, such as deploying technical experts, and provides assistance to decision makers
- Sustainability measures – training, exercising, and evaluating on a continuous cycle and maintaining resources and personnel to ensure effective use of measurement and assessment capabilities
- Knowledge management – retaining useful data (e.g. radiation signatures, site configurations, equipment lists) that help detection and reachback experts learn from past experience adjudicating alarms

• Participants also discussed the value of developing a gamma spectra repository or library where experts could securely share spectral and associated metadata. Additional relevant information could be added to the library such as a list of common detection equipment, and gamma analysis software for countries looking to establish their detection and reachback capabilities.

Future proposed work

This envisioned presentation could highlight priorities for future collaborative efforts related to reachback support, including the use of the definition and the core list of capabilities to further promote the development of reachback support in IAEA member states.

State
- Other

Gender
- Male

Primary authors: GALY, Jean (European Commission / Joint Research Centre); MAYER, Klaus (European Commission - Joint Research Centre, Institute for Transuranium Elements); TAGZIRIA, Hamid (European Commission, Nuclear Safety and Security Directorate, Nuclear Security Unit)

Presenter: GALY, Jean (European Commission / Joint Research Centre)

Track Classification: CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
Stumbling Block in Transport Security – Uncovering The Reality

Gap analysis from two (2) of recent cases involving Iridium-192 industrial radiography sources that were stolen during transit after completion of work and on transportation back to the main office from field work had shown that there is a strong need to enhance regulatory control and compliance efforts from authorised user on security of radioactive sources during transportation. The Atomic Energy Licensing Board (AELB), as national regulatory body has taken steps to improve security plan requirements that emphasis on the need to strengthen transport security for mobile radioactive sources in Malaysia. The regulatory improvement also focusses at enhancing synergy between transport safety and security within regulatory process and control. Among the important effort made was exploring better mechanism in tracking the movement of high mobility radioactive sources in Malaysia including the potential use of tracking technology. AELB took the important steps in consulting the authorised users and manufacturing industries to seek better understanding on cost effective solution within the available local technology in strengthening transport security implementation for mobile radioactive sources. Through our observation, it is obvious that the enhancement of transport security, will not be successful through depending only to the improvement of regulatory requirements. Such effort requires active and equal role and participation of all relevant competent authorities that has legal jurisdiction in managing and responding towards matter related to radioactive sources in transport, the authorized users and the manufacturing industry that are producing radioactive sources used in industrial radiography activities. the coordinated approach of competent authorities and relevant stakeholder will set for collective move in addressing issues and challenges involving technology availability, cost effectiveness, compliance with relevant international standard including quality control that will influence the successful and sustainable implementation in securing mobile radioactive sources. Acknowledging the limitation of genuine technology advancement for both radioactive source equipment manufacturing and the tracking capability in Malaysia, AELB works with the International Atomic energy Agency (IAEA) and other international cooperation partner to explore suitable and economical solutions before conditions specifically on tracking mechanism availability are made to the industry, in order to improve transport security control holistically. In this approach, the involvement of local industry is deemed to be highly necessary and important in ensuring compliance and control can be initiated directly from the core of the issues; the radioactive source itself.

State

Malaysia

Gender

Male

Primary authors:  Mr MOHD TAHAR, Rozman (Atomic Energy Licensing Board); BAKRI, Noor Fitriah (Atomic Energy Licensing Board (AELB))
**Presenters:** Mr MOHD TAHAR, Rozman (Atomic Energy Licensing Board); BAKRI, Noor Fitriah (Atomic Energy Licensing Board (AELB))

**Track Classification:** PP: Transport of nuclear and other radioactive material: practices, challenges and regulatory issues
Protection of Major Public Events against the Radiological Terrorist Threat: The Users’ Perspectives

As is widely recognised, there is not always a direct threat concerning the misuse of RN-materials during the planning of a major public event or whilst a major public event is in progress. However, if the competent security authorities deem it necessary, mobile radiation detection technology can be deployed at major public events. The radiation detection capability can be deployed by a supporting authority integrated into the security operation, for instance a radiation protection authority, or it can be deployed directly by the security authority itself.

The method of deployment of mobile radiation detection technology during a major public event varies depending on the type of detection deemed necessary by the competent security authority and on the type of equipment available. The strategy should be based on a threat and risk assessment for the major public event. For instance, the strategy could focus on the search for and detection of open and sealed nuclear and other radioactive material out of regulatory control before and/or during a major public event.

The European Commission has recently launched a new project, supported by DG HOME (EC Directorate General Migration and Home Affairs) to provide support enhancement of efficient networking and capacity building, offering EU Member States the opportunity to train representatives of their law enforcement national agencies in a state of the art facility to provide them with knowledge and hands on experience on how to detect and respond to the presence of nuclear materials in their field activities. One of the main activities is to support the transfer and the dissemination of knowledge necessary to spread rigorous nuclear Security Culture to the EU Members States. Under this scope, a workshop on securing major public event has been organized to share among EU Members states experience on training or on the use of dedicated detection equipment and technique in the frame of protecting a major public event.

The discussions highlighted lesson learned in, among others, planning and preparation for Nuclear Security Measures, tactics and approaches for deploying mobile detection technologies, assessment of information alerts and radiation detection instrument alarms, coordination with fixed equipment deployments, coordination with other national authorities and competencies, and the critical role of training.

This envisioned presentation will describe major outcomes from the users’ perspective.

State

Other

Gender

Male

Primary authors: GALY, Jean (European Commission / Joint Research Centre); WOJTAS, Wiktor (European Commission / DG HOME)

Presenter: GALY, Jean (European Commission / Joint Research Centre)
Track Classification: MORC: Nuclear security as part of the security of major public events
Proposed Nuclear Security Inspector Qualification Program

The Nuclear Energy for Peace Act 2016 (BE2559) delegates nuclear and radiation regulatory authorities to Office of Atoms for Peace (OAP). Article 107 of this act empowers OAP designated inspectors with regulatory oversight and early phase enforcement activities. However, this act does not allow nor specify the qualifications of these designated inspectors. Hence the Government Administration Act 1991 (BE2534) must be used as reference for setting up the requirements for inspector qualification program and system to be used in OAP. In this work, various inspector qualification systems from well developed countries have been reviewed in order to design new OAP’s inspector qualification program. It intends to differentiate type and specialization of inspectors, i.e. safety areas, security areas and safeguards areas. The proposed program divides interested personnel/inspectors into 3 levels, Pre-inspector, Junior inspector and Senior inspector. Competence, i.e. Knowledge, Skills and Attitudes (KSA) required to comprehend by each type and level of inspectors have been identified. Study of major aspects of the proposed changes to the program such as advantages and disadvantages when implement the proposed program has been performing as well as finding the solutions to smoothen the change process. The aim is to seek as much information in all areas to support the decision making in the organization.

State

Thailand

Gender

Female

Primary authors:  SRIMOK, Boonchawee (Office of Atoms for Peace); Mrs WATCHARASURAGUL, Varaporn; Mr SUDPRASERT, Somjait; Mr SUTRAPAI, Pisit

Presenter:  SRIMOK, Boonchawee (Office of Atoms for Peace)

Track Classification:  CC: National nuclear security inspections: training of inspectors, development of procedures and managing findings
Performance of a novel gamma-ray imager for nuclear security applications

Gamma-ray and neutron imaging technologies have many potential applications in nuclear security, safeguards, waste management and decommissioning. In particular, gamma-ray imaging enables one to remotely locate, identify, and quantify gamma emitting radionuclides, including Naturally Occurring Radioactive Materials (NORM), industrial, medical or special nuclear materials (masked or shielded). These technologies can provide crucial information for the development of an efficient decommissioning plan, a survey of an area at a nuclear facility and a secondary inspection of a passing cargo at border crossing, amongst other applications.

There are varying types of imagers, each one with its own capabilities, strength and weaknesses namely coded aperture imagers, Compton imagers and compressive imagers with rotary masks. Gamma-ray imaging can be made with technologies that have different capabilities such as energy resolution and efficiency, and many of our applications may demand one or the other characteristics. For example, a high resolution detector such as an HPGe (Hyperpure Germanium) can only be grown and produced in small sizes crystals and thus would have lower efficiency compared to large volume but lower resolution NaI (Sodium Iodide) detectors. Depending on the radiation field and situation to be investigated and imaged, one would need to use one imager type or another and sometimes several. The development of a good graphical user interface, software for spectral analysis and decision making, are also important aspects when considering radiation imaging technologies.

Previously, twelve imaging technologies were demonstrated and tested for safeguards application during a workshop organized by the IAEA at the Seibersdorf laboratories in 2015, from which a report was drafted by the Joint Research Centre (JRC). In the field of nuclear security, and within the technical subgroup of the Border Monitoring Working Group, the JRC organised a week long measurement campaign (in May 2017) to assess the capabilities and performance of five different gamma-ray imagers in a number of nuclear security scenarios. It was shown that systems could not easily be comparable as they had quite different performance capabilities. Earlier from 2012 to 2014, within an EU funded project (SCINTILLA), a CZT based gamma-ray imager was tested at the JRC as part of a tool box to develop systems for the detection of difficult to detect nuclear and radioactive materials as well as He-3 free radiation portal monitors. All of the above activities and projects, and many others, have shown good progress in the maturity of the gamma-ray imaging technologies, developed initial testing procedures/assessments and thus contributing to technology development and innovation.

This paper describes the performance of a gamma-ray imaging system that satisfies some if not most of the above requirements for use in nuclear security particularly, but also in nuclear safeguards and decommissioning. In essence, the system is based on the theory of compressed sensing and employs rotary masks that perform compressive measurements and considerably reduces the number of measurements (and time) required to reconstruct an image. The described imager can image a wide energy range over a wide field of view. Emphasis will be given to nuclear security applications to combat the illicit trafficking of nuclear materials and other radioactive sources out of regulatory control. The development of testing and assessment procedures for imagers, which would lead to better standardisation as performed within the ITRAP+10 project for all available families of radiation detection instruments, shall also be reported on.

State
Italy

May 9, 2020
Gender

Male

Primary authors:  Dr BOARDMAN, David (Australian Nuclear Science and Technology Organisation (ANSTO)); Mr ROZITE, Arturs (EC-JRC); Dr GUENETTE, M (ANSTO); Dr CHARTIER, L (ANSTO); Dr FLYNN, Alison (ANSTO); Dr BARNES, J (ANSTO); ILTER, J. (ANSTO); KARANTONIS, N (ANSTO); PETKOVIC, L (ANSTO); PROKOPOVICH, D (ANSTO); SARBU TT, A (ANSTO); WATT, G (ANSTO)

Track Classification:  MORC: Detection technology development and performance testing
Coordinated Response and Practical Aspects to Nuclear Security Events in Albania.

In Albania, radioactive sources are used in medicine, industry, agriculture, research and teaching process. The basic law for radiation protection in the Republic of Albania is the law "On Protection from Ionizing Radiation ", No. 8025, date 09.11.1995, and also, Law. 9973, date 28.07.2008 "On some amendments and additions to Law no. 8025, dated 09.11.1995 " On Protection from Ionizing Radiation", that approximates the IAEA safety fundamental, which establishes basic safety standards to protect health of workers and the general public environment against the dangers arising from the ionizing radiation.

Radiation Protection Commission (RPC) as the Regulatory Body defines the policies related to the treatment of the radioactive waste and DSRS in collaboration with other institutions. The Radiation Protection Office (RPO) is established as the executive body of the RPC. Institute of Applied Nuclear Physics (IANP) is the institution responsible for the processing and management of all radioactive waste and DSRS, produced in Albania and also of the orphan sources.

In support of safe and secure radioactive materials management and transport a Memorandum of Undertaking no.419 dated 14.01.2009 has been signed between General Customs Directorate and IANP with the aim "For detecting and combating of illicit trafficking on radioactive materials" where is reflected co-operation between institutions, when radioactive materials beyond prescribed norms are determined, technical assistance for the control and prevention of illicit trafficking of radioactive materials and continuous training of front line officers.

In implementation of the Albanian legislation in force, aiming at the protection and security of these types of materials, the response against their illicit trafficking, not only for criminal purposes, but also the consequences of the loss of control over radioactive sources, is approved the regulation "On Standard Procedures of Operations (SOPs) for the detection of radioactive materials "of the General Customs Directorate.

In order to secure the border to prevent the unauthorized entrance - exit and transit of the radioactive sources in the Republic of Albania, the Albanian Customs Service has taken all the due measures to place the necessary devices for automatic and/or manual detection of the radioisotopes in border crossing points. The allocation of such devices should make possible to detect and/or identify strength/nature of source and should be realized in line with the establishment of functional response plans/ procedures prepared by the Customs Service in cooperation with RPC and IANP.

This paper will discuss the present situation on the responsible institutions cooperation to ensure the safety and security in response to nuclear security events in Albania.

State
Albania

Gender
Male

Primary author: Dr PRIFTI, Dritan (Institute of Applied Nuclear Physics)
Co-authors:  Prof. BYLYKU, Elida (Institute of Applied Nuclear Physics); Dr DACI, Brunilda (Institute of Applied Nuclear Physics); Dr TUSHE, Kozeta (Institute of Applied Nuclear Physics)

Presenter:  Dr PRIFTI, Dritan (Institute of Applied Nuclear Physics)

Track Classification:  MORC: Coordinated response to nuclear security events
Implementing a Tabletop Exercise (TTX) for assessing PPS’s efficiency in National Center for Scientific Research “Demokritos”

The paper describes the conduction of a tabletop exercise at the premises of NCSR Demokritos, in order to examine the efficiency of the Physical Protection System against external adversaries. The work forms part of the activities of the group within the framework of the IAEA CRP J02006 “Enhance the Effectiveness of Nuclear Security at Research Reactor and Associated Facilities” and in particular Task 1 that assessed methodologies developed by the NUSAM CRP as applied to RRAFs. The objectives of the TTX were 3-fold:

• Contribute to the continuous training of Security Personnel at N.C.S.R. Demokritos,
• Evaluate the implementation of Security Procedures and the Response by Security Personnel during an Emergency Scenario that included external threats,
• Determine the Weak Points and Vulnerabilities in the PPS and the Security Procedures of the facility.

Implementation

For the implementation of the TTX, the Sandia TTX Methodology was used. The TTX took place in 2 daily workshops. Participants were exclusively selected by N.C.S.R. Demokritos Security Personnel. They were divided in two Teams, Red Team (adversaries) and Blue Team (protective forces). Red Team picked up their attack scenario. Their weapons characteristics were chosen from a list of available equipment. They had also to select types of vehicles. Blue Team manned their ordinary posts and followed the Emergency procedures already established, using their everyday operational equipment and vehicles. For the purpose of the TTX, all the appropriate charts described in Sandia TTX Methodology were used. Also charts depicting Access Delay Times in fences/gates, Penetration Times in walls/doors, Cutting Rates, Probability of Detection and all the necessary info described in RTC 2016 on Physical Protection of Nuclear Material & Nuclear Facilities training material, were advised.

Comments

Upon TTX completion, enough time was devoted for a thorough discussion between the participants and the organizing team focused mainly in comments, proposals and upgrades concerning the existing PPS and its Safety Procedures.

Acknowledgments

The authors would like to thank S.K. Hill, and G.A. Baum from Sandia National Laboratories for their valuable contribution during the design of the exercises.

State

Greece

Gender

Male
Primary authors: Mr TSOUROUNAKIS, IOANNIS (N.C.S.R. "DEMOKRITOS"); Dr SFETSOS, ATHANASIOS (N.C.S.R. "DEMOKRITOS"); Mr KOVATSOS, KONSTANTINOS (N.C.S.R. "DEMOKRITOS"); Mr XINTAVELONIS, IOANNIS (N.C.S.R. "DEMOKRITOS")

Presenter: Mr TSOUROUNAKIS, IOANNIS (N.C.S.R. "DEMOKRITOS")

Track Classification: CC: Good practices in the development and execution of nuclear security exercises (e.g. tabletop, drills and field exercises);
Methodologies and approaches useful for Cyber Threat Assessment and Cyber DBT along side with classical DBT methodology as stated in NSS-10 Document

Nuclear power plants and other nuclear facilities are considered among the most critical infrastructure assets vulnerable to cyber attacks leading to loss of lives, property destruction and economic upheaval. It is essential that these cyber threats be properly addressed considering their nature of risk at particular nuclear facilities. The classical methodology described in NSS 10 document for Physical threat assessment and physical DBT may not be sufficient to cover all the cyber threats due to a few differences in physical and cyber threats as described below.

The classical physical threat assessment process as described in NSS-10 document, starts with the identification of adversaries in the location of nuclear facility. Once you know the active adversaries, the investigating agencies and other stakeholders involved in the DBT assessment process, find out the characteristics of adversaries like Motivation, intension and capabilities. These characteristic data of adversaries is further analyzed in threat assessment and DBT process to get the most probable and realistic threat vectors against which the physical protection is designed and implemented to ensure the highest physical security for the nuclear facilities and nuclear power plants.

The differences in physical and cyber threats:

1. Cyber threats are a global phenomenon not only local.
2. It is not possible to know all the cyber adversaries, as they are spread all over the glob and not open or known in public as in physical adversaries.
3. No intelligent agencies can find out their characteristics like capabilities and intensions, as they are not open or known.
4. Cyber adversaries are location independent as they can attack from any where in the globe, which makes the task of intelligent agencies further difficult.
5. Cyber threats are more technology intensive than physical threats so as the technology advances, cyber threats are also becoming more advance. Cyber threats are more dynamic as compare to physical threats, which are more constant without much advancement in weapon technologies.
6. Cyber skill can be easily available and purchased or can be acquired in short time. So it is difficult for investigating agencies to clearly find out the capabilities of known cyber adversaries.
7. Cyber threats can be easily carried out without any deterrent (as in physical protection) as adversaries are always hidden. So cyber threats are more dangerous. It makes more essential to implement cyber threat assessment program more rigorously.
8. Cyber resources used in attack are easily available in the open market without any restriction and can be purchased without any issue and large funds as compare to physical resources.

Points 6,7 and 8 make the investigating agencies task more complex and difficult as with this adversary can develop the capabilities in very short time.
The NSS-10 document does not provide enough guidance to derived effective cyber security threat assessment and cyber DBT. The model of physical protection is not easily applicable to cyber defense. Moreover, describing the cyber threat landscape is not an easy undertaking, as has been discussed in several computer security consultancy meetings at the IAEA. The design-basis-threat approach (DBT) as described in NSS 10 is insufficient to cover cyber threat problem. The Paper presentation will discuss the approach and methodology of cyber security threat assessment and cyber DBT in the nuclear sector. It will provide practical ideas on the development of a cyber threat assessment and cyber DBT along with its impact and challenges.

State
India

Gender
Male

Primary author:  Mr PARULKAR, Sanjay Kumar
Presenter:  Mr PARULKAR, Sanjay Kumar

Track Classification:  CC: Information and computer security considerations for nuclear security
Urban Radiological Accident Mapping Using Smartphones Equipped with Personal Radiation Dosimeter

Nuclear safety and nuclear security are two subjects that they should be considered in the field of nuclear science and nuclear technology. Radionuclides can be released to the environment due to unforeseen accidents and incidents. The releasing of radionuclides decreases the level of safety and security of states. Radiological contaminations may happen during nuclear and/or radiological accident in nuclear facilities or form materials out of regulatory controls. Hence, contaminated regions in urban and suburban may have resulted from nuclear and/or radiological accidents. These regions can lead to the expose of members of the public to ionizing radiation resulting in negative health effects in the exposed population. According to the life-saving strategy during emergencies, it is necessary to characterize the contaminated region on map within 2-3 hours after starting accident, especially in the regions that there is high level of population. Environmental assessment during radiological accident need large amount of data. In order to investigate, control and regulate a contaminated region the possibility to perform screening surveys of the contaminated region using in-situ techniques is an important alternative allowing to improve the safety of people and to reduce the costs of the contamination survey using traditional instruments. In this research improvement of national nuclear safety and nuclear security using personal Smartphone that equipped with dosimeter during nuclear or radiological accident is considered.

METHODOLOGY

New generation of personal radiation dosimeters that can be attached to Smartphone has been developed by manufactures. It is possible that the national nuclear emergency centers provide radiological contamination map using personal Smartphones and national Wireless Communication System and/or WiFi (Fig. 1).

Fig. 1 Images of some commercial radiation dosimeter attachable to smartphones.

RESULTS

During the radiological accident in urban and suburban, nuclear emergency center need complete information about the contaminated region, movement and transformation of radiological contamination. The evacuation criteria after a nuclear or radiological accident needs a vital decision that involving risk-benefit should be done by decision makers to make a decision within hours. For the procedure of evacuation, the geographical direction and the radiological map of region is essential. To have a trustable radiological map, the environmental monitoring must be done with high efficiency and fast techniques. Due to development of technology, application of many kinds of techniques in environmental monitoring has increased during the last years. The first step of radiation mapping in a region is choosing the proper radiation detectors. Before selecting an instrument, it is important to understand both the activity concentration values that are to be verified, the capabilities of the monitoring instruments and the characteristics of the potentially contaminated material. Some types of instruments are quite expensive, a factor that may limits their availability for radiological mapping. For the measurement strategies one should determine the most likely affected environmental compartments and probable migration pathways. Such specifics have to be taken into account to make a proper selection of the devices needed to investigate the contaminants of concern by performing in situ measurements.

Now a days, some manufacturers have produced several kinds of personal dosimeters that can be attached to the Smartphone. The Smartphone are used in all countries and near the all of people have their own Smartphone. Hence, it is possible for people to have a personal dosimeter that attached to their Smartphone for their lifetime. Handling of personal dosimeter by people have many advantages. In this research we would like to study the application of personal dosimeter
during urban and suburban nuclear or radiological accident. The software or app that installed in the Smartphone can manage the attached dosimeter. The Smartphone can present the radiation dose rate and the accumulated radiation dose using Wireless Communication System. If the received radiation dose rate is more than background radiation, the Smartphone can give an adequate alarm to aware the owner of the Smartphone. The online Smartphone can send two significant data to the national nuclear emergency control center using Wireless Communication Systems. The first is the geographical position and the second is radiation dose rate of related geographical position intervally. Using the received date from each Smartphone, the data collection system can provide online radiation map of region and present to decision makers.

State

Iran

Gender

Male

Primary authors: Dr NABIPOUR CHAKOLI, Ali (Nuclear Science and Technology Research Institute, AEOI, Tehran, Iran); MASSEY, Charles (IAEA)

Presenter: Dr NABIPOUR CHAKOLI, Ali (Nuclear Science and Technology Research Institute, AEOI, Tehran, Iran)

Track Classification: CC: Innovative technologies to reduce nuclear security risks and improve cost effectiveness, where feasible
Sustaining and Strengthening Efforts for Nuclear Security in Azerbaijan

The possibility that nuclear or other radioactive material could be used for malicious purposes cannot be ruled out in the current global situation. Given that this problem is global, the contribution of each state is very important for achieving a common goal. In this regards, the necessary efforts are being made in Republic of Azerbaijan to strengthen the protection and control of such materials and to respond effectively to nuclear security events. The creation of appropriate regulatory bodies, the improvement and development of legislation and regulations, the introduction of a graded approach to control, as well as participation in various international projects and the development of international cooperation make an invaluable contribution to the development of existing infrastructure. However, as in many areas, along with achievements in ensuring state control and supervision over the security of radioactive materials, there are also difficulties associated with the need to continuously improve the knowledge and professional training of staff, improve the material and technical base, introduce advanced technologies, etc. Taking into account the above, the paper will consider both the existing practice and taken measures for sustaining and strengthening efforts for Nuclear Security in Azerbaijan.

State

Azerbaijan

Gender

Male

Primary author:  PASHAYEV, Ramin (Head of Department on Special permission and State registry of the State Agency on Nuclear and Radiological Activity Regulations (Regulatory Authority) of the Ministry of Emergency Situations of the Republic of Azerbaijan)

Presenter:  PASHAYEV, Ramin (Head of Department on Special permission and State registry of the State Agency on Nuclear and Radiological Activity Regulations (Regulatory Authority) of the Ministry of Emergency Situations of the Republic of Azerbaijan)

Track Classification:  CC: Implementation of national legislative and regulatory frameworks, and international instruments
Considerations for regulatory body: Nuclear security culture self-assessment

Security culture self-assessment plays a key role in developing and maintaining an awareness of the strengths and weaknesses of Nuclear security culture (NSC). IAEA recently published technical guidance NSS No. 28-T (Self-assessment of Nuclear Security Culture in Facilities and Activities). Self-assessment is not strictly confined to the operators’ side but also to regulators’ side. However no self-assessment of NSC in regulatory bodies and technical support organizations (TSOs) have been published so far. However the required tools for culture self-assessment can be found in IAEA NSS No. 7 and No. 28-T; they just have to be tailor-fitted to the needs of the regulatory body. The regulatory body plays a central role here, taking his self-reflection about his own role modelling into account. So the paper is focused on some considerations for regulatory body about nuclear security culture self-assessment for the evaluation of the current state of the security culture and for the derivation of an action-plan to strength sustainability and effectiveness of nuclear security regime.

Considerations
- The main challenge consists in selecting appropriate characteristics from the generic IAEA model to be able to tailor-fit a suitable bunch of indicators in the second step. The next crucial step deals with fitting a bunch of suitable statements with unambiguous and understandable messages. Performing such a campaign should therefore lead to a deeper understanding of the security culture and its importance for an effective security regime.
- The self-assessment for the regulator should be easily understandable and applicable so that it may affect any level of inspector in an effective and efficient way. In addition the self-assessment survey should be limited and focused to appropriate topics and not try to cover all the indicators in the above mentioned IAEA publications.
- Some characteristics are playing a central role for the regulator, such as work environment, training and qualification, effective communication, motivation, professional conduct and adherence to procedure whereas other areas seem to be of minor importance for the regulator himself, e.g. improving performance, expectations or performance measurement.
- The special challenges of regulatory body are including the limited control regulatory body have over their goals, the presence of subcultures, and the nature of the interaction between the regulator’s organizational culture and those of the nuclear facilities and associated activities. One key task of a regulator is to influence and shape the cultures of the nuclear facilities and associated activities so that they better advance policy goals. As a result, regulatory leaders interrelated challenge of trying to manage their own organizational culture in ways that enable them to both infer and influence the cultures of the nuclear facilities and associated activities cultures.
- As in the area of nuclear safety assessment, security culture assessment must balance between self-assessment with and without the involvement of outside specialists, as both modes have their advantages and disadvantages. Self-assessment team members possess in-depth knowledge of the organization, its people, its processes, and key influences. They are insiders and therefore have a stake in, and are more accountable for, improvement. Safety and security must reinforce one another in pursuing the common objective of protecting people and the environment.
- It’s important to understand the distinct differences between security and non-security personnel are vital to a balanced and accurate assessment as well as to corrective management arrangements.
- Nuclear security culture training of competent authority representatives may enable them to better observe and identify indicators of a strong nuclear security culture and assess gaps that need to be addressed.
- A self-assessment may be conducted at the beginning of implementing a programme for the enhancement of nuclear security culture and may be regularly repeated in order to assess the current nuclear security culture within an organization.
-Quality assurance can contribute to a strong nuclear security culture. Nuclear security needs a high degree of rigor, control and assessment to remain effective. Therefore, well-documented and applied quality assurance practices for nuclear security will help ensure its effectiveness.

- Continuously developing a common understanding of security culture and establishing a positive dialogue with the licensee is of primary importance for performing effective regulatory oversight of security culture.

- Implementation of National capacity building programs for nuclear security, that need the involvement of all stakeholders, including regulatory bodies, nuclear operators, technical support organizations, law enforcement agencies, and organizations responsible for responding to nuclear security events. The cooperation and coordination of these stakeholders are critical for the optimization of the program to be effective in meeting national needs of nuclear security capacity building. National knowledge networks for nuclear security are the basis for such cooperation, coordination and sustainability.

State

Egypt

Gender

Female

Primary author:  ELABD, Amira (Egyptian Nuclear and Radiological Regulatory Authority (ENRRA),)

Presenter:    ELABD, Amira (Egyptian Nuclear and Radiological Regulatory Authority (ENRRA),)

Track Classification:  CC: Nuclear security culture in practice with a focus on sustainability
Preliminary Fuel Development and Reactor Design Milestones for the LEU Conversion of the U.S. High Performance Research Reactors

The continued presence of highly-enriched uranium (HEU) fuel in civilian installations such as research and test reactors poses a threat to national and international security. Minimization, and ultimately elimination, of HEU in civilian research and test reactors worldwide has been a goal of policy in many countries, including in the United States, since 1978. In order to reduce the threat posed by HEU while allowing the facilities concerned to continue operating and achieving their important and diverse missions in science and medicine, conversion to low-enriched uranium (LEU) fuel often requires the development of high uranium density fuel to compensate for the enrichment reduction.

The United States Department of Energy / National Nuclear Security Administration (DOE/NNSA) Reactor Conversion Program is working collaboratively with many countries worldwide towards the conversion of remaining reactors to the use of LEU fuel. Conversion of civilian research reactors from HEU to LEU, and the return of the HEU to the country of origin is an important component of the NNSA non-proliferation program. Worldwide, 71 reactors have been converted to the use of low-enriched uranium (LEU) fuel, and an additional 28 have been confirmed to be permanently shut down. These 99 reactor conversions include 20 U.S. reactors among the 39 countries on six continents where conversions have occurred. With two recent conversions in Africa, in Ghana and Nigeria, this completes an important milestone. Africa is the third continent to have completed all HEU to LEU reactor conversions, following Australia and South America. For the remaining conversions in Europe, the U.S. and elsewhere, reactor conversions underway commonly require higher density fuel and qualification under more extreme conditions.

For the six U.S. high-performance research reactors (USHPRR), NNSA has developed a very high-density uranium-molybdenum (U-10Mo) alloy LEU fuel that would allow the conversion of all the facilities. This paper will discuss the fuel development milestone that has been completed, leading to a Preliminary Report on U-Mo Monolithic Fuel for Research Reactors submitted to the U.S. Nuclear Regulatory Commission (NRC) in 2017. This was accomplished in addition to a Preliminary Design Milestone for each of the USHPRR reactors where each reactor’s unique fuel element was re-designed from 2010 to 2018. Three Preliminary Safety Analysis Reports for conversion to LEU fuel were submitted have to the U.S. NRC by the National Institute of Standards Reactor (NBSR), the University of Missouri Research Reactor (MURR), and the Massachusetts Institute of Technology Reactor (MITR). The DOE-operated Advanced Test Reactor (ATR), and the associated critical assembly (ATRC), and High Flux Isotope Reactor (HFIR) reactor have also completed preliminary designs with U 10Mo fuel. However, an opportunity to convert HFIR using uranium silicide fuel at, or near, the standard density used worldwide has been made possible using a longer fuel plate and advanced design techniques. For HFIR, silicide fuel is now being pursued for LEU conversion, along with the fuel qualification testing required at higher power densities than is currently available, and, like HFIR requires today, for a contoured fuel design including boron in the plate.

Continuing efforts are required following these Preliminary USHPRR Milestones. Using the commercial fabrication pilot line that has been installed and is currently operating, full-size fuel plates and assembly fabrication are planned to perform qualification irradiations and flow testing that will ultimately lead to USHPRR conversions to LEU fuel.

State

United States
Gender

Not Specified

Primary authors: WILSON, Erik (Argonne National Laboratory); Dr COLE, James (Idaho National Laboratory); Ms DUNN, Kerry (Savannah River National Laboratory); LAVENDER, Curt (Pacific Northwest National Laboratory); Mr CERCY, Micheal (Savannah River National Laboratory)

Presenter: WILSON, Erik (Argonne National Laboratory)

Track Classification: PP: Minimization, on a voluntary basis, of high enriched uranium within civilian stocks and where technically and economically feasible
A Policy Study Using Self-Assessment Tools to Assess Thailand’s Readiness and to Strengthen National Nuclear Security Regime

In 2018, Office of Atoms for Peace (OAP) conducted a policy study to consider approaches and measures appropriate for Thailand’s current situation on nuclear security as well as conforming to international legal instruments and standards. The research team led by the then OAP Deputy Secretary-General executed a study with qualitative methodology including literature reviews, gaps analysis by using IAEA self-assessment tools, in-depth interviews with key persons involving with national security and/or nuclear security, assessment of national nuclear security capabilities. The study aimed to evaluate nuclear security needs and priorities as well as draw significant results and recommendations to strengthen the national nuclear security regime.

The initial tool used in this study was literature reviews of international instruments related to nuclear security. The team studied various information sources such as the United Nations Security Council Resolutions, IAEA Nuclear Security Series, and relevant treaties and conventions. The reviews also covered a holistic view of national nuclear security regime as well as an implementation of public policy.

In the meantime, OAP cooperated with nearly twenty intragovernmental organizations to identify gaps and needs by using the IAEA-developed self-assessment tool, Integrated Nuclear Security Support Plan (INSSP). Through a support by the IAEA experts and national workshops, Thailand officially submitted the INSSP to the IAEA in April 2018. The INSSP has initiated the implementation of nuclear security activities that are now functioning according to the plan. After INSSP submission, OAP updated online information of Thailand’s nuclear security status in Nuclear Security Information Management System (NUSIMS) to make it consistent with the INSSP. It is noted that both IAEA-developed self-assessment tools, INSSP and NUSIMs, were useful and informative mechanisms to complete this work.

Since this is a policy study, assessment of national nuclear security capabilities was rather essential to take into account. The team studied the key responsibilities of OAP and national authorities such as Police, Military, National Security Council, etc. to see a whole picture of national nuclear security legislative framework. Moreover, the team requested to interview policymakers and experts from national authorities and IAEA to pull together different points of view to push forward Thailand’s nuclear security regime.

The results from the study showed many strengths as well as several downsides of Thailand’s nuclear security. Specific policies were drawn from these results through six measures including legislative and regulatory measure, threats and risk assessment, physical protection, detection of criminal acts, security response and sustainability. The results will be postulated as a recommended implementation plan in a form of OAP nuclear security roadmap and will be reflected in the national security policy hereafter. The results also provide insightful information for a project grant proposal related to national nuclear security. The details of how Thailand conducted a self-assessment study to strengthen national nuclear security regime will be explained in this paper.

State

Thailand

Gender
Primary authors:  KASIWATTANAWUT, Haruetai (Office of Atoms for Peace, Thailand);  Mr TU-LARAK, Thitidej (Office of Atoms for Peace, Thailand);  RUEANNGOEN, AREERAK (OFFICE OF ATOMS FOR PEACE);  Ms TANJOY, Vilaivan (Office of Atoms for Peace, Thailand)

Presenter:  KASIWATTANAWUT, Haruetai (Office of Atoms for Peace, Thailand)

Track Classification:  CC: Identification of national needs through the development of an Integrated Nuclear Security Support Plan
Activities and Challenges of Nuclear Security within the Forum for Nuclear Cooperation in Asia (FNCA)

In response for to the diversification of energy resources, several Asian countries have currently considered nuclear power as an option. As a result, a dramatic increase on the use of nuclear material is foreseen; nuclear security and safeguards, as well as nuclear safety, will become more important in the promotion of the peaceful uses of nuclear energy. For these reasons, the Nuclear Security and Safeguards Project (NSSP) started in 2011 within the framework of the FNCA, aims to cooperate with FNCA member countries to strengthen their respective infrastructures. The FNCA is a framework led by Japan’s Cabinet Office and the Ministry of Education, Culture, Sports, Science, and Technology (MEXT) for international cooperation with neighboring Asian countries towards the peaceful uses of nuclear technology. The framework for FNCA cooperation consists of a Ministerial Level Meeting, Senior Officials Meeting, Coordinators Meeting, and a Study Panel. The participating 12 countries are Australia, Bangladesh, China, Indonesia, Japan, Kazakhstan, Korea, Malaysia, Mongolia, the Philippines, Thailand, and Vietnam. Currently, 7 topical projects are being conducted with collaborative activities under equal partnership in various nuclear fields. Each project promotes joint research, discussions on common challenges, and information exchange. A workshop is held annually. Conversely, the Integrated Support Center for the Nuclear Nonproliferation and Nuclear Security (ISCN) of the Japan Atomic Energy Agency (JAEA) has been providing assistance, specifically to Asian countries. Therefore, the ISCN has closely collaborated with the NSSP.

The objectives of the NSSP are to share experiences, knowledge, and information on nuclear security and safeguards implementation including human resource development (HRD) and research and development activities. In 2015, under the NSSP, a survey was conducted among FNCA member countries on future activities. At the 6th FNCA workshop in 2016, the results of the survey and the prospects for future activities were discussed. The following fields were selected for this project: 1) Nuclear Security: Nuclear forensics, cyber security, nuclear security culture, and security of radioactive sources. 2) Safeguards: Additional Protocol, others. 3) Common for security and safeguards: Capacity building under Centers of Excellence (COEs)). The 19th FNCA Ministerial Level Meeting (MLM) was held in Japan, on December 2018. The MLM Joint Communique reiterated and emphasized the FNCA’s objectives toward the peaceful uses of nuclear technology. The accomplishments of the NSSP activities have shown the importance and beneficial effects of the collaborative efforts among the FNCA member countries. This paper describes a 3-year plan and the outcome, and also challenges of the NSSP activities.

State

Japan

Gender

Male

Primary authors: Mr SENZAKI, Masao (INMM Japan Chapter); Ms RODRIGUEZ, Perpetua (JAEA); Dr
SEKINE, Megumi (JAEA); Mrs KIMURA, Yoshiki (JAEA)

**Presenter:** Mr SENZAKI, Masao (INMM Japan Chapter)

**Track Classification:** CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
Nuclear security education as a tool to sustain nuclear security regimes

Nuclear security is fundamental in the management of nuclear technology and in applications where nuclear material or other radioactive material is used or transported. It is the responsibility of the states to establish, maintain and sustain effective nuclear security regimes. Every state’s regime comprises of a set of policy and technical nuclear security measures. It is essential to have well educated and qualified people capable of implementing these measures to ensure that the national nuclear security regime is effective and efficient.

Universities worldwide understood the needs and have established nuclear security academic programs. This initial education provides students with deep knowledge and understanding of nuclear security. Only, very few universities have developed a full nuclear security master program. Other universities have opted for incorporating nuclear security modules as part of their education program for nuclear scientists and engineers. As a result, the graduates will be qualified to serve in nuclear security jobs or they can conduct research activities in nuclear security. This will help to work on emerging threats and emerging technologies to advance nuclear security globally.

The International Nuclear Security Education Network (INSEN) has supported faculty members and researchers in establishing their academic courses and offers an excellent platform for international cooperation on nuclear security education and research. It is clear that the number of courses at the universities has increased significantly these last years. However, most of these courses, especially in developing countries, don’t include practical work, which hampers the students’ full understanding of technical nuclear security measures.

This paper will describe how nuclear security education can contribute to sustaining nuclear security regimes – talking about some opportunities and challenges. It will also discuss the importance of establishing collaborations between universities and Nuclear Security Support Centre (NSSC), when it exists, for better developing a national human resource strategy and research activities.

State
Morocco

Gender
Female

Primary author: Prof. HAKAM, Oum Keltoum (University of Ibn Tofail, Morocco)
Presenter: Prof. HAKAM, Oum Keltoum (University of Ibn Tofail, Morocco)

Track Classification: CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
The practice and exploration of radiation detection equipment performance testing work carried out by China Customs

In order to maintain good international and domestic order and prevent and combat illicit trafficking in nuclear and other radioactive materials, in recent years, China Customs has been equipped with a large number of radiation detection equipments throughout the country. And China Customs has been carried out radiation detection work at national water, land, air and passenger entry and exit ports. China Customs nuclear radiation detection work started in 2008, which originated from the security needs of the Beijing Olympic Games. The first batch of equipped radiation detection equipments came from various sources, including the unified distribution of independent procurement by China Customs, free donation by equipment manufacturers and donation by third-party organizations. China Customs used these equipments to carry out nuclear radiation detection work at border ports. After years of work, China Customs has summarized the Practice and exploration about using these equipments to carry out nuclear radiation detection work at border ports. China Customs has constantly summarized the achievements and shortcomings of nuclear radiation detection work. In order to facilitate the further and detailed development of nuclear radiation detection work, China Customs has put forward some individualized requirements for the performance of radiation detection equipment, which needs to be tested before purchasing new equipment. In 2016, China Customs invited a number of international and domestic agencies such as radiation detection equipment manufacturers, China National Atomic Energy Agency and the National Laboratory of the United States Department of Energy and other international or domestic institutions to participate in the performance testing work of equipment. This is the first time that the China Customs has systematically tested the performance of radiation detection equipment used in the Customs system. 

This paper first introduces the individualized requirements of the nuclear radiation detection work of China Customs, and then introduces the practice and exploration of the performance testing work of the radiation detection equipment used by China Customs. Contents include the aspects of the preparation, operation specifications, technical indicators and performance evaluation of the equipment testing work, summarizes and experiences of the performance testing work of the radiation detection equipment. The innovation of this paper is that China Customs innovatively puts forward the individualized requirements for radiation detection equipment. For the first time, it systematically carries out the performance test of equipment, and records the specific situation of the test work. It is not only a summary of the experience for China Customs, but also more importantly, it can provide experience for other countries.

Keywords: China Customs, radiation detection equipment, performance testing

State
- China

Gender
- Male
Primary author: Mr ZHAO, Bin (Chinese Academy of Customs Administration)

Co-authors: Mr ZHAN, Jian (Chinese Academy of Customs Administration); Mr LIU, Hong (Chinese Academy of Customs Administration)

Presenter: Mr ZHAO, Bin (Chinese Academy of Customs Administration)

Track Classification: MORC: Detection technology development and performance testing
The practice and exploration of nuclear security education and capacity building about China Customs

Compared with developed countries such as the United States and Russia, China Customs has less experience in nuclear radiation detection work at its border ports. Its technical ability and equipment are relatively backward, and there are deficiencies in its work, especially in nuclear security education and capacity building. In terms of self-construction, there is less talent reserve for nuclear radiation detection posts, limited resources and capabilities for post skills training, and there are many areas worthy of improvement. In recent years, the China Customs Radiation Detection Training Center which cooperative constructed by China and the United States has been completed and put into operation. It has organized radiation detection skills training for China Customs and other countries in the Asia-Pacific region. It has trained personnel in nuclear radiation detection posts for China Customs and national Customs in the Asia-Pacific region, and has accumulated some advanced practices in education and post training. In particular, in recent years, in order to implement the spirit of the President of the People’s Republic of China Xi Jinping’s speech at the Fourth International Nuclear Security Summit, the China Customs Radiation Detection Training Center assisted the IAEA in organizing radiation detection skills training for national first-line officer radiation detection skills training. And then providing intellectual support for international nuclear security capacity-building.

This paper starts with the specific practice about the training of nuclear radiation detection skills in China Customs Radiation Detection Training Center, and introduces the exploration and practical experience of the China Customs in the construction of national nuclear security capacity building include the content about the perspectives of training program, curriculum, teachers training and training management. The innovation of this paper is that the paper introduces the specific methods and practices of China Customs nuclear security capacity building from the perspective of trainers, and introduces how to make better use of the teaching methods such as desktop deduction, practical drills, situational teaching and other teaching methods in training. The way of confrontation increases the pertinence, authenticity, and interest of nuclear security training. How to scientifically arrange courses in training, increase the comprehensiveness of teaching content, and how to improve the quality and ability of teachers systematically and continuously. What methods are used to improve training efficiency and save training costs. How to carry out media publicity to raise the importance of citizens’ attention to nuclear security work and other issues, so as to provide Chinese Customs and other national Customs with the experience of building nuclear security capacity that can be used for reference.

Keywords: China Customs, nuclear safety education, capacity building

State
China

Gender
Male
Primary author: Mr ZHAO, Bin (Chinese Academy of Customs Administration)

Co-authors: Mr ZHAN, Jian (Chinese Academy of Customs Administration); Mr LIU, Hong (Chinese Academy of Customs Administration)

Presenter: Mr ZHAO, Bin (Chinese Academy of Customs Administration)

Track Classification: CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
Good practices in the joint drills on nuclear security at border ports between China Customs and neighbouring countries

Customs is the administrative department of the state to exercise the authority of border port entry and exit supervision and administration, and Customs is the first line of defense to guard the security of the country. Customs plays a very important role in maintaining national security. China Customs attaches great importance to nuclear security, earnestly implements the state’s main responsibility on nuclear security, fulfills the functions and powers conferred by the law, and continuously strengthens border port nuclear radiation detection work. In recent years, China Customs has continuously strengthened international cooperation in border port nuclear security with Russia, Kazakhstan and other neighboring countries. China Customs invited cooperative countries to participate in nuclear radiation detection work at border ports and send personnel to participate in seminars, training courses and bilateral cooperation projects related to border port nuclear radiation detection work in cooperating countries. China Customs and the Russian Customs Administration have established a long-term cooperation mechanism. Each year, holding annual meetings of the Sino-Russian Customs Joint Working Group on the Prevention of Illicit Trafficking in Nuclear and Other Radioactive Materials. The minutes of the meeting are signed by the two sides for the implementation of annual cooperation projects and make the cooperation plan for the next year. Since 2015, China Customs and the Russian Customs Administration have organized a joint drill to prevent illicit trafficking in nuclear and other radioactive materials every year. They have already successively held joint drills at Chinese Heihe border Port on 2015, at Russia’s Bragovishinsk border Port on 2016, at Chinese Manzhouli border Port on 2017 and at Russia’s Begalsk border Port on 2018, and on 2019 the joint drill will be held at one border port of China. China Customs has accumulated rich experience in joint drills of nuclear security at border ports. In addition to cooperation with the Russian Customs Administration, China Customs is carrying out the nuclear security cooperation with other neighbouring countries. At present, China Customs is planning to cooperate with Kazakhstan Customs in organizing a joint drill to prevent illicit trafficking in nuclear and other radioactive materials. This paper discusses the specific practice of formulating and implementing joint drills on nuclear security between China and Russia, either between China and Kazakhstan. It introduces the purpose of bilateral cooperation between two countries, the planning and preparation of joint drill on nuclear security, and the best practices of joint drills on nuclear security at border ports between two countries. The innovation of this paper is to provide other countries with the best practices that can be used for reference in bilateral cooperation on nuclear security at border ports between the two countries.

Keywords: China Customs, border ports, nuclear safety joint drill

State

China

Gender

Male
Primary author:  Mr ZHAO, Bin (Chinese Academy of Customs Administration)

Co-authors:  Mr ZHAN, Jian (Chinese Academy of Customs Administration); Mr LIU, Hong (Chinese Academy of Customs Administration)

Presenter:  Mr ZHAO, Bin (Chinese Academy of Customs Administration)

Track Classification:  CC: Good practices in the development and execution of nuclear security exercises (e.g. tabletop, drills and field exercises);
Investigation of radioisotope source masking effects on uranium gamma-ray spectra in determining of 235U abundance in uranium samples

Abstract

In nuclear technology, one key parameter is the uranium enrichment of the uranium material for the characterization. For quick and accurate determination of uranium enrichment at border checkpoints to prevent illegal trafficking and contraband of special nuclear materials, such as uranium or plutonium, gamma-ray spectrometry is a fast and cheaper tool than other analytical tools due to its ease of use, portability, non-destructive nature for determination of the isotopic uranium abundance. From point of nuclear material security in the nuclear security activities, it is well known that gamma-ray spectrometry is a versatile technique and it allows analysts or FLOs(front of lines) or first responders on-site to measure and identify the radiation sources and materials. However, the uranium enrichment necessitates the use of specifically designed instrumentation and methods. In this study, for the correct identification of depleted uranium(DU), natural uranium(NU) and low enriched uranium(LEU) samples, the masking effects of the medically/industrially used radioisotopes have been investigated on uranium gamma-ray spectra, which were taken by LaBr3:Ce, CdZnTe and HPGe detectors, respectively. In practice, especially in transportation of radioactive materials or radioisotope sources, the nuclear materials can be masked by other radioisotopes such as 241Am, 57Co, 133Ba, 152Eu, 99mTc and other medically used radioisotopes. In such circumstances, the presently available algorithms used for the de-convolution of the peaks in the acquired gamma-ray spectra have some deficiencies to de-convolute the close lying peaks and thus the calculated peak areas for the analytically used peaks can result in erroneous results in the uranium enrichment determination.

In this study, two intermediate energy resolution detectors that are a 38.1mmx38.1mm LaBr3:Ce scintillator with a resolution of FWHM=2.7%@662 keV(137Cs) and a 15mm x 15mm x 7.5mm CdZnTe semiconductor with a resolution of FWHM=2.5%@662 keV(137Cs) and a high resolution(FWHM=0.575keV@122 keV(57Co)) portable, LN2 cooled and HPGe (its crystal has 37.7mm in diameter and 16.4 mm in thickness) were used in the experiments. As a uranium material, depleted, natural and low enriched uranium( U3O8) samples having the enrichment of about 0.32 to 4.51% atom 235U certified reference materials (EC-NRM171 sealed cans) obtained from EU-JRC IRRM were used. From the acquired uranium spectra, the enrichment values of the samples were determined two different analytical approaches: one is uranium enrichment meter principle(EMP) that uses 185.7 keV peak of 235U and the other is multi-group gamma ray analysis (MGA) that uses very closely appeared x-ray and gamma-rays, which are lying in 80-130 keV low energy region of uranium spectrum. In the experimental setup parameters, each detectors was installed in a radiometric bench in which the uranium source sample and the detector was aligned with a laser light and measured the source-to-detector distances. In each detector setup, firstly, lead collimators and interleaved absorbers(aluminium and iron) between sample and detector were placed to observe the effects on the accuracy 235U isotopic abundance in uranium samples. Then, at a given source-to-detector geometry, the different radioisotope sources ( such as 241Am, 57Co, 133Ba, 152Eu, 99mTc, 232Th) are, in turn, counted together with uranium sample in a sealed aluminium can to simulate the masking conditions, where the chosen radioisotope source was, respectively, placed at the lateral sides, back side and front side of it in order to observe the scattering effect of uranium in the Al-can. The spectra analyses of the uranium materials masked by other radioisotope sources
were made COLEGRAM and with a newly developed spectrum de-convolution algorithm based on the modified Figure-of Merit (m-FOM) under MATLAB platform. This algorithm can be easily applicable to EMP. In MGA analysis, U-235View(Ortec) and Genie MGAU (Canberra) commercial softwares were used. These programs are applicable to the uranium gamma-ray spectra taken by a high resolution HPGe detector. The differences between the calculated enrichment values and the reference values of 235U at different worst measuring conditions were generally found to be less than 15%. The differences become much lower in favorable conditions such as long counting time, ideal detector-sample distance. However, in case of the uranium spectra masked by other radioisotope source or materials, the interpretation of discrepancies in the 235U enrichment results will be discussed in detail in the presentation.

State
Turkey

Gender
Male

Primary author: Prof. YÜCEL, Haluk (Ankara University, Institute of Nuclear Sciences)

Co-authors: Mr BALCI, SEFER (Ankara University, Institute of Nuclear Sciences); Ms SAATCI, SELIN (Ankara University, Institute of Nuclear Sciences); Ms KAPLAN, NESLİHAN CEREN (Ankara University, Institute of Nuclear Sciences); Ms BARUT, AYŞEN (Ankara University, Institute of Nuclear Sciences, Tandogan Campus, 06100 Ankara, Turkey); Mr YELTEPE, Emin (Ankara University, Institute of Nuclear Science); Mr NARTTURK, Recep Bora (Ankara University Institute of Nuclear Sciences); Mrs GUVEN, Rufiyet (Ankara University, Institute of Nuclear Sciences)

Presenters: Prof. YÜCEL, Haluk (Ankara University, Institute of Nuclear Sciences)

Track Classification: MORC: Detection technology development and performance testing

May 9, 2020
Page 226
Strengthen Computer Security on Radiation Detection Equipment for Nuclear Security

Radiation detection equipment is very important as its purposes used for nuclear security need in the prevention intentional and unintentional unauthorized acts involving nuclear and radioactive material. And computer security is a particular aspect of information security that is concerned with computer based systems, networks and digital systems. Normally people focus attention on the specific conditions affecting computer security at nuclear facilities follow NSS-17. But IAEA documents about computer security on radiation detection equipment is little while technical and functional specification of equipment, which may directly relate to the detection results, is well-known as NSS-1.

Since each procedure of relative detection data is expected to be digital in current digital age, hidden dangers of juggled digital data will affect the accuracy of equipment performance and mislead monitoring results of nuclear radiation detection. All fields of security (including personnel, physical, information and computer) interact and complement each other to establish an equipment’s security. A failure in any of the field could impact the other. Computer security on radiation detection equipment is a cross-cutting field that has interactions with all on-site practical security factors.

In this paper two aspects, where one is technical control and the other is management, are primary considered to be strengthened to effectively protect information security of control computer. The content includes extending performances related with computer security to technical and functional specification of equipment. This may protect digital data on computer (including embedded singlechip), communication system and connected cable from cyber-attack.

From the aspect of technical measures, the primary means of preventing and mitigating the consequences of security breaches is "defence in depth". Since a radiation detection equipment is an integrated system with detecting, transmitting, processing and storing functions, the digitization of data from detector is start of control flow. Then according the composition of the equipment, flow direction of digital data need to be controlled. Also access control ways such as encryption of files, identification of authorization, remote access restrictions and necessary authentication can be adopted. Communication protection can be enhanced from digital feature composition of hardware and protocols of software. It is better if a tamper-proof mechanism for data files can be established.

From the aspect of management control, a security policy of regular inspection should be established. Its context cover life cycle management of a radiation detection equipment, including data of continuous monitoring, records of software operating, adjusting, controlling and processing, logs of different operators. When there is exceptional case, it may means the equipment has the risk of out of control. If possible, assessment tool can be used to conduct vulnerability assessment tests such as vulnerability scanning and Trojan penetration on the system of equipment.

State

China

Gender

Male
Primary authors:  Prof. LI, Yong; Prof. WANG, Guobao; Prof. WANG, Qiang

Presenter:  Prof. LI, Yong

Track Classification:  CC: Information and computer security considerations for nuclear security
Improving the Efficiency of Use and Increasing the Resource of Physical Protection Inspection Equipment - the Role of Training Courses for the End User

The most important characteristics of the radiation monitoring equipment used to ensure Nuclear Security are: reliability, stability in operation, maintainability, repairability, long life of the system. To achieve these indicators, in addition to the quality assurances declared by the equipment manufacturer, an important role is played by the culture of operation and maintenance of on-site inspection systems. Personnel who use and maintain inspection equipment must have the appropriate qualifications, primarily the necessary knowledge of its principles of operation, design and maintenance. In this regard, to conduct high-quality education and training of the end staff is of fundamental importance.

This paper summarizes the experience of conducting training for personnel who operate and maintain inspection equipment for physical protection: radiation monitoring equipment, determinants of explosives, and integrated inspection systems - both at Russian enterprises and within the framework of the IAEA programs. Based on the experience gained, the following conclusions are made:

1. The need for staff training at different levels is shown: • • Training of first line officers (operators) - response to alarms generated by equipment. In particular, for the alarms generated by radiation monitoring systems, the primary separation of “innocent alarms” caused by natural or medical isotopes; • • Training of service personnel - carrying out routine and periodic maintenance, scheduled inspection of basic functional characteristics. On-site small repair skills training (e.g. possible replacement of faulty modules from the spare parts kit); • • In-depth theoretical and practical training with the provision to students of all technical documentation, including electrical circuits, allowing for the repair of any complexity without the involvement of representatives of the manufacturer.

2. The impact of the quality of the learning process on the effectiveness of the results is evaluated. In the educational process, in addition to lectures and visual material (presentations, video courses), it is necessary to use technical means: real equipment nodes of a specific manufacturer, which allow reproducing possible faults and practical training of personnel in their elimination. This contributes to the development of practical skills and leads to an improvement in real results.

3. The efficiency of training is shown not only in specialized centers, but also on the basis of the manufacturer, and, especially, directly at the facilities where equipment is located, that is, the workplaces of personnel. In this case, learning takes place on the same equipment that is actually used in work. The specifics of the specific place of use and equipment operating conditions are taken into account.

State
Russian Federation

Gender
Male
Primary author: CHUVAEV, Sergey (SEC "Nuclear Physics Research")
Presenter: CHUVAEV, Sergey (SEC "Nuclear Physics Research")
Track Classification: PP: Physical protection systems: evaluation and assessment
Nuclear security education efforts to develop the next generation in Morocco

Morocco is an active member of the IAEA and has signed all the protocols and conventions relating to nuclear security and the non-proliferation. Since 2016, Morocco has created its regulatory authority for Nuclear and Radiological Safety and Security and has continued to undertake activities to establish a reliable nuclear security program concerning the use of radioactive sources and nuclear material used in Morocco or in its region. These activities include efforts by the most Moroccan universities and existing training centers to include nuclear security and non-proliferation courses in masters programs and the development of training programs for professionals.

The University of Ibn Tofail in Morocco is one of the forerunners in this field, having established its educational programme at an early stage in 2010, while taking into account the need for faculty development courses (FDCs) for national, regional and international participants, as well as student’s needs for theoretical and practices oriented programmes.

Equipped with experiences of previous courses and capacities within the country, Morocco requested to hold the first regional school on nuclear security held in French, based on the joint IAEA-ICTP International School on Nuclear Security.

In this presentation, we will talk about some main activities undertaken by the University of Ibn Tofail in collaboration with national and international universities and organizations:

1- The introduction of nuclear security and non-proliferation courses in the Master’s programs in Radiation Protection and Nuclear Science and Technology. These courses cover the various topics of nuclear security such as the national nuclear security regime, the culture of nuclear security, the transportation and management of radioactive sources, information security and cyber security,

2- proposal of the subjects for the projects of end of studies in master cycle which relate to exercises and scenarios of nuclear security,

3- organization of a regional nuclear security school by university of Ibn Tofail in collaboration with the IAEA for young professionals from African countries speaking French with contribution of experts from IAEA, Morocco and other countries and organizations,

4- organization of some workshops, round tables and exercises for academics, students and professionals in nuclear field.

5- Successful associative work within the framework of Student INMM chapter created for the first time nationally, regionally and continentally by University of Ibn Tofail. this association has ensured the organization of activities on nuclear security in several national universities and institutes.

State
Morocco

Gender
Male

Primary author: Prof. CHOUKRI, Abdelmajid (Universiy of Ibn Tofail)
Presenter: Prof. CHOUKRI, Abdelmajid (Universiy of Ibn Tofail)

Track Classification: CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
Additional Protocol Implementation in Industries That Produce Technologically Enhance Naturally Occurring Radioactive Material (TENORM) in Indonesia

Indonesia is a country rich in natural resources, both metal and non-metallic mineral resources, including tin and zircon. The by-products of tin and zircon processing still contain valuable minerals such as ilmenite, rutile, monazite and pyrite with a significant amount. However, the by-products of tin and zircon processing have the potential to have high radiation exposure compared to normal exposure. This is caused by the content of natural radionuclides contained in it, such as U-232 and Th-232. In addition, to being obliged to administer storage permits (BAPETEN Chairman Regulation, BCR No. 9-2009 and BCR No. 16/2013), businesses are also required to report the source material (Uranium and Thorium) content they have (BCR No. 9-2006 and BCR No. 9-2008). This is also requirement from the International Atomic Energy Agency by INFCIRC 153/ Add.1 and INFCIRC 540.

The purpose of this paper was to explain the interface between Technologically Enhance Naturally Occurring Radioactive Material (TENORM) and implementation of additional protocols in industries that produce TENORM in Indonesia.

BAPETEN did monitoring, verification, licensing and inspection of TENORM. The currently subject of TENORM supervision was tin and zircon industries in Indonesia. BAPETEN also reported to IAEA, the containing of uranium and thorium annually with additional protocol declaration. Based on BAPETEN supervision, tin and zircon industry produce by product that contain source materials consist of uranium until 0.09% and thorium 2.5%. The radionuclides concentrations were 6.2-18.4 Bq/gram thorium and 1.0 – 7.2 Bq/gram uranium. The industries equipped with security personnel, detection system, barrier and permanent inventory.

Keywords: additional protocol, TENORM, material source, security.

State
Indonesia

Gender
Male

Primary authors: Mr YOGA, Bhakti Dwi (BAPETEN, Directorate of Licensing); Ms INDIRANI, Deshinta (BAPETEN, Directorate of Inspection); Ms YULIATI, Evin (BAPETEN, Directorate of Licensing)

Presenter: Mr YOGA, Bhakti Dwi (BAPETEN, Directorate of Licensing)

Track Classification: PP: Nuclear material accounting and control
Evaluation of Computer Security Culture for Nuclear Security in Malaysia’s Medical Institution

It is important to have a robust computer security culture in order to enhance the efficiency of security plan since computer security culture is one of essential part of overall security culture. With a constant innovation on information technologies (IT), IT advancement can be utilized to develop a more composed security management through building, maintaining and even promoting awareness on computer and information security. This indirectly will strengthen the existing nuclear security in every medical institution available. The study is aimed to identify the effectiveness of computer security culture in organization’s culture and improvement that can be made. Several medical institutions has been chosen as a location for the research which is Universiti Kebangsaan Malaysia Medical Centre, Ampang Hospital, Universiti Sains Malaysia Hospital, Advanced Medical & Dental Institute and Gleneagles Intan Medical Centre. The research was then assessed through questionnaires, interviews, observations and document review. From the results, even though majority of the staff are aware of computer security culture, they still didn’t embraced the computer security culture due to lack of security awareness and risk perception to the potential threat. There are various improvement initiatives can be done to provide more guidance to medical staff on managing sensitive and personal security information such as conducting an extensive training programme, initiating a bilateral exchange forum and coordinate a comprehensive seminar session. Besides that, a specific program called insider threats program can also be introduced to manage classified information and has ability to conduct thorough verification for all licensees that in charge on sensitive nuclear information categories under non-classified. In conclusion, computer security requirements are clearly documented and are in place but the security culture is not practiced by all staffs and are not well understood by staffs.

State

Malaysia

Gender

Male

Primary author: MOHD KAMARI, MOHD NATHIR (MINISTRY OF HEALTH MALAYSIA)

Presenter: MOHD KAMARI, MOHD NATHIR (MINISTRY OF HEALTH MALAYSIA)

Track Classification: CC: Information and computer security considerations for nuclear security
Global nuclear security depends strongly on the efforts of international organisations and leading donors, combined with an efficient regional coordination and solid national commitment. While there are several initiatives addressing CBRN risks from different angles, there are few which follow an integrated CBRN approach, despite the definite added value of such a strategy (for example in the coordination of response agencies and front line officers). The EU CBRN Centres of Excellence (EU CBRN CoE) is one of the only global initiatives to pursue an integrated CBRN risk mitigation, with proven success. The EU CBRN CoE initiative addresses risks related to CBRN material and agents of any origin: criminal (proliferation, theft, sabotage and illicit trafficking), accidental (industrial catastrophes, in particular chemical or nuclear, waste treatment and transport) or natural (mainly pandemics but also consequence of natural hazards on CBRN material and facilities). This approach reinforces the countries’ competences in addressing the CBRN risks not only in a strictly security-related scenario but also in other settings of accidental or natural occurring releases, which enhances the sustainability and endurance of the developed capacities.

The network structure supported by the EU CBRN CoE is also a factor of sustainability: the country hosting the EU CBRN CoE Regional Secretariat designates the Head of the Regional Secretariat, and all Partner Countries of the region designate nominate a National Focal Point and a CBRN National Team, which forms a coordinating and information-sharing working group between the different national institutions involved at various levels in national CBRN risk mitigation. The National Team members provide their experiences from agencies involved in the country’s preparation and response in the different CBRN fields, discuss national coordination and, particularly, enhance the relevance and ownership of the implementation of capacity building activities. The involvement of the European External Action Service and of the EU Delegations is a crucial factor of success of the initiative. Also, administrative support and contribution for diplomatic coordination is ensured by staff of the United Nations Interregional Crime and Justice Research Institute (UNICRI).

One of the first activities implemented by the Initiative at national level is an integrated needs assessment in CBRN, with the effective participation of the National Focal Point and of the National Team. This is also an opportunity for a preliminary discussion of CBRN risks among the national delegates and for the mapping of other existing CBRN initiatives in the country. This exercise allows for the identification of areas for improvement where actions should be taken and, together with a risk assessment component, is the basis for the formulation of a National CBRN Action Plan (NAP). The NAP is an essential tool for national authorities to articulate priorities and coordinate the implementation of a comprehensive national strategy against CBRN risks for the medium to long term, where the capacity building activities should be nested.

The EU CBRN CoE capacity building activities are tailored to the needs of the individual countries but with a regional dimension, and resort to different mechanisms: revision of the national regulatory framework addressing CBRN risks, training of operational officers, train the trainers of programme coordinators, field and table exercises or demonstrations, networking of existing or new infrastructures and deployment of interoperable, feasible equipment.

In summary, the EU CBRN CoE strategy for promoting sustainability in global CBRN security is the adequate combination of a well-supported bottom-up needs assessment, a consistent network of National Focal Points and National Teams in constant dialogue, the development of a government-endorsed CBRN NAP, the implementation of impactful and well-coordinated projects and a strong
local ownership of the capacity building activities.

**State**

- Other

**Gender**

**Primary authors:** Dr GOULART, Margarida (European Commission - Joint Research Centre); Dr ABOUSAHL, Said (European Commission); GONÇALVES, Mariana (European Commission - Joint Research Centre); OCEANO, Ivana (European Commission - Joint Research Centre); Ms SANTOPOLO, Daniela (European Commission - Joint Research Centre); Ms FIETZ, Katharina (European Commission - Joint Research Centre); Ms SZUCSOVA, Kristina (European Commission - Joint Research Centre); Ms FEDERICI, Ilaria

**Presenter:** Dr GOULART, Margarida (European Commission - Joint Research Centre)

**Track Classification:** CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
EMBARKING THE JOURNEY- NUCLEAR SECURITY IN MAJOR URBAN AREAS

The record has shown, 84% cases of material out of regulatory control in Malaysia were contributed by mobile radioactive sources. From the figure, 38% were reported missing while another 38% were reported stolen. In both cases, almost 64% incidents occurred during transit with 68% incidents contributed by the Industrial Radiography Activities. At present, Malaysia has over 90 registered companies in Industrial radiography activities deals with more than 500 category 2 industrial radiography sources. At the latest nuclear security event where one industrial radiography source went missing during transportation, the Government had instructed to include control mechanism involving detection of nuclear and radioactive materials as part of security screening activities to the national scale event such as celebration of National Independence Day 2018 and National Sports Games 2018. Due to growing concern on cases involving industrial radiography sources, Malaysia revise approach towards management and preparedness focusing on major urban areas where some of activities involving radiography sources frequently take place. The main concern is on the potential radiological, economical and sociological consequences in the event if the material falls to the wrong hands of innocent people with limited knowledge on radioactivity or to the individuals with malicious intention. Geographically, the mobile material that goes out of regulatory control could lead to potential effect of transboundary to other major urban cities including to the cities across Malaysia’s border. Learning from experience in securing major public events that was first implemented during visit of President Barrack Obama to Malaysia in 2011 followed by the 2017 South East Asian Games organized at major urban cities, Malaysia had extended the experience in developing such capability for detection at major areas conducted through joint operation between Atomic Energy Licensing Board (AELB) and the Royal Malaysia Police (RMP). In developing nuclear security capability for major urban areas, AELB played a major role in extending technical expertise in supporting RMP for the development of an integrated Standard Operating Procedures (SOPs) for detection and response. The integrated SOP leveraged the existing capacities and functions from both RMP and AELB to jointly address nuclear security threat at major urban areas. Training programmes were also designed and implemented to enable RMP’s roles for detection at major urban areas by incorporating nuclear security functions to their daily duties with strong focused in enhancing detection by information capabilities. Limited number of detection equipment were also distributed with priority given to police forces in major urban areas and in identified strategic location with volume of radiation activities take place. The concept of information, expertise and asset sharing is applied as strategic approach to build detection capabilities at major urban areas in light of limited resources to ensure a sustainable and effective program availability.

State

Malaysia

Gender

Male
Primary author: BIN RADZUN, Hatman Riza

Co-authors: Mr MOHD TAHAR, Rozman (Atomic Energy Licensing Board); BAKRI, Noor Fitriah (Atomic Energy Licensing Board (AELB)); Mr MUHAMMAD JAMIL, Muhammad Zul Azri; AB. RAHIM, Mohd. Hafizi; Mrs PUNGUT, Noraishah (Atomic Energy Licensing Board (AELB))

Presenter: BIN RADZUN, Hatman Riza

Track Classification: MORC: Nuclear security in major urban areas
Safety and Security Interface: The Implementation on the Transport of Nuclear Materials and Radioactive Sources in Indonesia

Safety and Security Interface: The Implementation on the Transport of Nuclear Materials and Radioactive Sources in Indonesia

E. Yuliati1, D.Sinaga1,
1 Nuclear Energy Regulatory Agency (BAPETEN), Jakarta, Indonesia
E-mail address of main author: y.evin@bapeten.go.id

Abstract. Indonesia is archipelago country with large area. The large use of radioactive materials in all over Indonesia needs serious attention on the safety and the security of the transport of these materials. Nuclear Energy Act No. 10 year 1997 article 27 mentions that the transport shall regard the safety of workers and public as well as the protection to environment. Particularly, government has issued Government Regulation (GR) No. 58 year 2015 on Radiation Safety and Security on the Transport of Radioactive Materials. In fact, there is interface between safety and security that needs adjustment in implementation of this regulation. The adjustment is based on potential threat that might arise. Therefore, there is a coordination of many institution involved before the transport. Indonesia has experiences in the transport of nuclear materials and radioactive sources. There are some cases of transport such as repatriation of spent fuel of research reactor, transport of imported nuclear material for research reactor fuel fabrication, and transport of radioactive sources from hospital to radioactive waste management facility. From those cases, it can be drawn lesson learnt on how to balance safety and security aspect in the transport of nuclear materials or radioactive sources.

Key Words: safety, security, interface, transport, radioactive source, nuclear material.

State

Indonesia

Gender

Female

Primary authors: Mrs YULIATI, Evin (Nuclear Energy Regulatory Agency); Ms SINAGA, Dahlia (Nuclear Energy Regulatory Agency)

Presenter: Mrs YULIATI, Evin (Nuclear Energy Regulatory Agency)

Track Classification: CC: Nuclear safety and security interfaces
Development of National Training Capabilities to Support Nuclear Security Infrastructure in Kazakhstan

The Republic of Kazakhstan is a strong advocate in the non-proliferation of nuclear weapons, being one of only four countries to give up nuclear weapons they previously had in their territory, and is a consistent supporter of the idea of peaceful use of atomic energy.

Kazakhstan has a rich nuclear heritage and developed nuclear infrastructure, including former nuclear test sites; uranium industry; low enriched uranium bank IAEA; BN-350 fast neutron power reactor under decommission; nuclear research centers with research reactors and radiochemical laboratories; industrial companies and medical centers using thousands of radioactive sources.

Nuclear technologies, widely used for industrial, medical and scientific purposes, are an integral and important part of the economy of Kazakhstan. Along with substantial economic benefits, these technologies also bring the risks of theft, sabotage, malicious use, and dissemination of sensitive information related to the use of nuclear and radiological materials. To mitigate these risks, Kazakhstan has introduced a nuclear security regime, the infrastructure of which includes the relevant legislative and regulatory framework, state authorities and operators implementing measures to ensure the physical protection of nuclear facilities, nuclear and radioactive materials, accounting and control of nuclear and radioactive materials, information security, measures to counter the illicit trafficking of nuclear and radioactive materials.

Sustainable and efficient functioning of the nuclear security infrastructure, coordinated interaction and improvement of all its elements require continuous development of human resources. Understanding the need for education and training of personnel in the field of nuclear security, at the 2012 Nuclear Security Summit, Kazakhstan announced its intent to establish a specialized training center.

The Nuclear Security Training Center (hereinafter - the Center) was constructed on the site of the Institute of Nuclear Physics through a cooperative effort between United States and Kazakhstan. The Center’s opening ceremony took place in May 2017.

Now Center provides training on fundamental aspects of nuclear security and provides a platform for discussing best practices in this area. The main areas of training at the Center are the physical protection of nuclear facilities and materials, the accounting and control of nuclear material, the combatting illicit trafficking of nuclear and radioactive materials, radiation safety, as well as information and cyber security. Since its opening, more than 300 specialists have been trained in the Center. Trainees represented Kazakhstan’s nuclear industry enterprises and nuclear research centers, state authorities, regulatory bodies, border guard and customs services, interior and national security agencies, and transport enterprises. The training courses conducted at the Center demonstrated the advantages of nuclear security training in a specialized center equipped with full-scale simulators, mock-ups and benches, a training ground and a transport checkpoint with modern equipment, same as equipment being used at real facilities.

In the framework of the Center’s establishment project, with methodological, technical and financial support of the National Nuclear Security Administration of the US DoE, the training needs analyzes were conducted, training materials for basic courses on physical protection (PP), accounting and control of nuclear materials were developed, instructor training courses and joint training courses on PP fundamentals were held. The Defense Threat Reduction Agency of the US DoD has conducted more than 10 training courses at the Center under the Global Nuclear Security Program. International cooperation, joint activities with partners contribute to the development of the Cen-
The Center has the opportunity to train not only the personnel of Kazakhstan organizations, but also specialists from other countries. For the sustainability of the Center, considerable efforts will still be needed to develop additional training programs, select and improve the qualifications of instructors, and improve the Center’s operational plan. Cooperation of the Center with international experts allows to effectively solve these problems. To participate in the international dialogue, the Center in 2017 became a member of the International Network of IAEA Nuclear Safety Training and Support Centers (NSSC Network).

The established Center is not only an element of national security, but also Kazakhstan’s contribution to strengthening global nuclear security.

**State**

Kazakhstan

**Gender**

Female

**Primary authors:**  Ms IZMAILOVA, Natalya (Institute of Nuclear Physics); Ms IDRISSOVA, Marzhan (Institute of Nuclear Physics)

**Presenter:**  Ms IZMAILOVA, Natalya (Institute of Nuclear Physics)

**Track Classification:**  CC: Role of Nuclear Security Support Centers to support and sustain national nuclear security regimes
EU technical activities contributing to global Nuclear Security

Through collective efforts, the international community has made great strides in creating and promoting global awareness and cooperation in nuclear security. Since the 1st Nuclear Security Summit in 2010, an increased awareness and political momentum favoured international cooperation and boosted initiatives and activities at the IAEA level, as well as in the framework of the Global Partnership Against the Spread of Weapons and Materials of Mass Destruction, the Global Initiative to Combat Nuclear Terrorism, Interpol, the current Nuclear Security Contact Group. In terms of cooperative processes, considerable progress has been achieved at international, national and regional level.

From a broad perspective, while raising awareness and boosting international cooperation, the wave that brought nuclear security high on the political agenda at international level also contributed to tangible achievements, by strengthening overall commitment in order to ensure that nuclear and radioactive materials are further secured - and in particular that prevention, detection and response to malicious acts is improved.

At the EU level, nuclear security lies with national governments and remains the sole responsibility of each Member State. However, due to its global connotation, to the interdependency of different risks and of the measures to face them, it is broadly acknowledged that coordination within the European Union, as well as international cooperation, will remain crucial.

Through the work of the European Commission’s Joint Research Centre (JRC), the EU provides valuable technical support including education and training, in alignment and complementarity with MS’ needs and activities, and also contributing to the international nuclear security framework.

This paper illustrates how the EU has integrated the efforts in global security at the top of its political priorities, in active cooperation with the IAEA and other relevant partners. Moreover, it presents the main technical achievements in key areas related to nuclear security. The technical nuclear expertise developed by the EC/JRC during 60 years and the valuable research carried on in the areas of detection, response and forensics, bring tangible results for enhancing EU internal nuclear security. This expertise, put at the service of EU MS, also serves the development of EU standards for detection technologies and forensic methodologies. Additionally, training and exercises provided in the framework of the European Nuclear Security Training Centre (EUSECTRA) represent key elements for an effective nuclear security system. Awareness raising, capacity building and outreach initiatives, deployed through the EU CBRN Centres of Excellence, are successfully performed in order to join forces at international level, harmonise approaches to prevention, preparedness and response for the mitigation of CBRN risks worldwide, as well as to maximise the results from collective efforts.

Together with the IAEA and other international and national partners, the EU supports - through its technical nuclear security expertise - the global nuclear security architecture and continues to play a crucial role in consolidating achievements and boosting new developments.

**State**

Other

**Gender**
Primary authors: ABOUSAHL, said (European commission); GOULART, Margarida (European Commission Joint Research Centre); OCEANO, Ivana (European Commission - Joint Research Centre); GONÇALVES, Mariana (European Commission - Joint Research Centre)

Presenter: ABOUSAHL, said (European commission)

Track Classification: CC: Advances in nuclear security research and development; international cooperation on nuclear security research
Implementing and Developing Nuclear Safety and Security Culture for Radioactive Material, Associated Facilities and Activities

The use of radioactive material is increasing rapidly all over the world for a wide variety of beneficial purposes, in industry, medicine, agriculture, research and education. There is, thus, need for safe and secure applications of radioactive material, and safety and security measures are protect and prevent from causing a radiological hazard on individuals, society and the environment. Myanmar has used radioactive sources in these sectors, are safely and securely controlled under the IAEA issued International Basic Safety Standards and Security Guidance. At present, Myanmar is implementing safety and security culture management for radioactive material, associated facilities and activities, and developing in safety and security culture on regulatory capabilities for National Regulatory Infrastructure.

National and international nuclear safety and security culture practices indicate that better prepare for, and mitigate the risk of, an attack or an accident by developing and implementing a harmonized approach to nuclear safety and security throughout all levels of an operation and organization. Nuclear safety culture means the assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, protection and safety issues receive the attention warranted by their significance, and nuclear security culture means the assembly of characteristics, attitudes and behavior of individuals, organizations and institutions which serves as a means to support and enhance nuclear security. Establishing a strong safety and security culture is one of the fundamental management principles for an organization dealing with radioactive material. All activities involving the use of radioactive material require careful attention to safety and security, and should be designed and implemented in an integrated manner, so that security measures do not compromise safety and safety measures do not compromise security.

In this proposal, presents implementing effective regulatory capabilities in using radioactive sources, associated facilities and activities, that developing by National legislation and international guidelines, using safety and security culture requirements promoted by IAEA. In Myanmar, Atomic Energy Law was placed in 1998 and to be more comprehensive for nuclear safety, security and safeguards; Nuclear Law is drafted and now, under processing. Currently, Division of Atomic Energy (DAE), established in 1997 under the Ministry of Science and Technology, is designated as a Regulatory Authority in comply with Atomic Energy Law, and performs all regulatory functions related to safety and security in utilization of radiation sources, radioactive material and irradiation apparatus. The sub–Division, Regulatory Control Division is assigned responsibility for law implementations, regulations, code of practices and rules, notification, registration, licensing, inspection, emergency response and preparedness, and law enforcement.

Myanmar has no nuclear fuel cycle facilities, power reactors or research reactors. The use of radioactive sources in medical, industrial, research and education, are imported and currently, total national inventory of radioactive sources is 857 with 796 facilities. In 2017, 220 active licenses across all sectors; industrial sector makes up 84%, healthcare services at 9% and the rest are research and education, issued licenses.

To control radioactive material, associated facilities and activities for safe and secure, DAE has the implementing internationally harmonized regulatory capabilities; Radiation Detection and Measurement Laboratory, Nuclear Instrumentation Laboratory, Occupational and Medical Exposure Laboratory, Non-Destructive Testing Laboratory, Gamma Irradiation Facility, Radioisotope Techniques Laboratory, Food and Environmental Monitoring Laboratory, Radioactive Source and
Waste Storage Facility, Secondary Standard Dosimetry Laboratory, and DAE provides Personal Monitoring Services, Technical Support and Guidance to radiation users, Environmental Monitoring, and conducts Export - Import Control through Atomic Energy Law, Emergency Preparedness, Training Programme, Public Awareness Programme, and is preparing to develop Physical Protection Plan, Code of Conduct for Safety and Security of Radioactive Sources, Radioactive Waste Management, Emergency Response Programme, Security Requirements, Technical Facilities including appropriate Equipment and Human Resources, and National Legislation. To improve the transparent activities in Nuclear Safety and Security Culture, Myanmar ratified International Convention on Nuclear Safety, acceded on December 6, 2016, Convention on Physical Protection of Nuclear Material, acceded on December 6, 2016, Comprehensive Nuclear Test Ban Treaty, acceded on September 21, 2016, and participates in the IAEA Integrated Nuclear Security Support Plan, and also to strengthen National Regulatory Infrastructure in Nuclear Safety and Security, Myanmar has cooperated with relevant national, regional and international organizations in Training, Workshop. Awareness and Culture Assessment play key roles in developing, maintaining, and enhancing nuclear safety and security culture, and benefit of harmonizing the two, ensures that threat and danger to the safety and security of operation are real, credible, and deserving of attention. Thus, to strengthen effective safety and security culture for radioactive material, associated facilities and activities in Myanmar, is trying to fill the gaps in national regulatory framework, technical facilities including appropriate equipment and human resources, national and international cooperation, financial supporting, and effective security culture management for radioactive material in use and disused sources storage, that will be supported to qualified assessments for nuclear safety and security culture on regulatory capabilities.

State
Myanmar

Gender
Female

Primary authors: Ms WIN, NWET NWET (Division of Atomic Energy, Ministry of Education); Mr LATT, KHIN MAUNG (Division of Atomic Energy, Ministry of Education)

Presenter: Ms WIN, NWET NWET (Division of Atomic Energy, Ministry of Education)

Track Classification: CC: Implementation of national legislative and regulatory frameworks, and international instruments
French approach of security by design: from the Opéra Garnier to SMR

On 14 January 1858, Napoleon III was victim of a bomb-attack in front of the Paris opera house by Italian terrorists as a response to French interventionism in their country. After this attack, Napoleon III decided the building of a new opera house that would be more prestigious but as well better secured: one of the most famous building in Paris was born, the Opéra Garnier.

Who remembers today that security was one of the concern of this building? If we look carefully, it clearly appears that security was considered as early as the design phase of the opera. This example will be used as an illustration of the benefits of security by design, in particular what is sometimes called “intrinsic security”.

To go further, we will explain how security by design principles used for the Opéra Garnier are still relevant for nuclear facilities. Three comparisons will be used:
- creation of the Avenue de l’Opéra, large enough to prevent any attack during travel time / integrated assessment of transport issues when considering the siting and design of a nuclear facility;
- “Rotonde de l’Empereur”, that provides a secured and dedicated access for the Emperor / underground design of SMR that provide protection against off-site attacks;
- direct access to the Emperor’s loge / reduction of the need to access vital area by moving consign- ment room from the main control room building to outside of the vital area.

These examples show how inherent features, integrated as early as possible during the design phase, contribute to enhance the security of the building regarding specific threats without the need to add dedicated physical protection systems afterward.

The current French approach of security by design can be resumed as a combination of:
- an intrinsically secured design, with inherent features of the installation that contribute to reduce the number of targets, to facilitate nuclear security and allow a better mitigation of the potential consequences of the remaining vulnerabilities and;
- an early identification of physical protection requirements, to cope with the vulnerabilities of the installation.

Security by design may also help to make easier the consideration of future changes in the threat during the lifetime of the installation. For instance, it can result in a design that provides rooms for future additional physical protection systems to cope with evolutions of the threat.

Therefore, in order to be as much efficient as possible, it is expected that designers take into account security aspects as early as possible during the design phase of the installation, as done for nuclear safety. However, one of the challenges for security by design is that it relies on a design basis threat which is specific to each country and is generally protected information.

Even though this approach has not been yet introduced in the regulatory framework, the French nuclear security authority is endeavoured to apply the principles resulting from the concept of security by design to new nuclear installations currently under construction or in development in France.

The list below is not exhaustive, but some principles that can be applied to new nuclear installations can be expressed as follow:
- how to optimize fuel assembly design and management to reduce vulnerability to theft?
- how to identify potential sabotage targets and reduce their numbers and/or vulnerabilities?
- how to optimize building organization and access to reduce opportunities for insider threat?
- how to adapt safety features, in particular passive features and/or redundancy, to face malicious acts as well?
- how to adapt transport provisions to reduce vulnerability of transports when accessing the site?

In conclusion, the concept of security by design, being a combination of an early identification of physical protection requirements and an intrinsically secured design, should be addressed as
early as possible by designers when developing new nuclear installations. It will result in facilities with more efficient and effective security, but also that are cost-effective with respect to threat evolutions and prevention of negative impacts on operations, safety, and safeguards.

**State**

France

**Gender**

**Primary authors:** LANGUIN, THOMAS (MINISTRY OF ENVIRONMENT, ENERGY AND THE SEA FRANCE); Mr DUCOUSSO, Erik (Ministry for an ecological and solidary transition)

**Presenters:** LANGUIN, THOMAS (MINISTRY OF ENVIRONMENT, ENERGY AND THE SEA FRANCE); Mr DUCOUSSO, Erik (Ministry for an ecological and solidary transition)

**Track Classification:** PP: Security by design, including in newcomer countries
Supporting carriers efforts to develop their security culture

Background:

Having a large nuclear industry imposes France to have a robust physical protection regime for the security of nuclear material, their facilities and their transport as well as a strong nuclear security authority. In this regard France reviewed its regulation and its Designed Basis Threat (DBT) from 2009 to 2011. However, to better adapt to the current threat, security adjustments are to be made. They have to be shared and fully understood by licensees so that security culture can be spread among all people in charge of or taking part to nuclear transports in their company. Here stands the real challenge.

Steps forward a better shared security culture

The threat is evolving. States and people have acknowledge that fact and governments are making their best to address it. The nuclear community does the same. Time has come to promote, develop, renew and harden security measures and processes to better answer it.

In this regard, the french nuclear security authority is supporting carriers’ effort to increase their security culture policy, among all personal in charge or connected with nuclear transports, in a continually improving process.

Different steps have already been taken. Further security stages have been initiated along the following trends:

- increasing the threat perception
- developing a transport security mindset among all the nuclear carriers community
- broadening the range of transport security inspections
- widening the “unpredictability program” on nuclear transports
- setting higher standards for nuclear transport licensees’ renewal.

This is the presentation the French nuclear security authority proposes to share and to elaborate on at the February 2020 security conference in Vienna. strong text

State

France

Gender

Primary authors: TERTRAIS, Christian (Ministère de l’énergie); Mrs JOLY, Claire (Ministry for an ecological and inclusive transition); Mrs GUYARD, Ophélie (Ministry for an ecological and solidary transition)

Presenters: TERTRAIS, Christian (Ministère de l’énergie); Mrs JOLY, Claire (Ministry for an ecological and inclusive transition); Mrs GUYARD, Ophélie (Ministry for an ecological and solidary transition)
Track Classification: CC: Nuclear security culture in practice with a focus on sustainability
Enhancing and maintaining unpredictability on nuclear transports

Background
Nuclear materials have to be secured while in facilities and during transports. It is a truism. That is why the CPPNM has been made and amended to fit with current threats. That is also the reason why IAEA is developing a set of NSS documents to help countries build, improve and implement their national nuclear security regime. The French nuclear security authority has emphasized the need to increase unpredictability on nuclear transports and developed a new concept.

Unpredictability strengthens security
Many constraints make difficult to conceal the occurrence of nuclear transports. On the one hand, safety is to be guaranteed and has to be made transparent to most of public opinions: Nuclear facilities are easily identified and steadily located, dedicated roads, rail tracks, harbours and airports are scarce and generally shared with public freight and passengers. Logistic organisation calls for reproducing the same transport scenarios schedules.

On the other hand, it is easily understood that security requires limited publicity and restrictions to keep days, hours, locations and length of stops, border crossing spots and itineraries of nuclear transports unknown.

That is the reason why, in 2017, France has initiated a strengthened unpredictability program. After a one year long experimentation implementation period, adjustments have been made to be fully operational since January 1st, 2019.

Unpredictability criteria at different stages of the transport
Unpredictability criteria to modified are well known: itineraries, night stops, temporary resting areas, days of departure / arrival, hours of departure and arrival,

Time has come to take stock of the currents achievements, to identify the lessons learned while implementing the whole process as well as to anticipate which could be the next orientations to keep the momentum of improving security in this area.

This is the presentation the French nuclear security authority proposes to share and to elaborate on at the February 2020 security conference in Vienna.
Presenters:  TERTRAIS, Christian (Ministère de l’énergie);  Mrs JOLY, Claire (Ministry for an ecological and inclusive transition);  Mrs GUYARD, Ophélie (Ministry for an ecological and solidary transition)

Track Classification:  PP: Transport of nuclear and other radioactive material: practices, challenges and regulatory issues
Insider threat and computer security: is there a specific profile?

In the infosec community, insider threat is a “buzz word” which covers several different meanings. However, in the nuclear field, IAEA has precisely defined it as “an adversary with authorized access to a nuclear facility, a transport operation or sensitive information”. Because many functions in nuclear facilities are now digitalized, computer networks are natural targets for a malicious actor and the agency’s definition of an insider can be applied to computer security.

In that aspect, “authorized access” can be broken down into two distinct domains:
- Physical access to a network equipment.
- Logical access to accounts/network functions.

Of course, to be able to generate a significant impact like a major denial of service, extraction of sensitive data or takeover of the industrial process, an adversary must gain a high level logical access (in technical terms, he basically needs at some point to become “root” or “admin”), hence the widespread belief that insiders, in the computer security field, must have a deep computer and network knowledge and a high level of access rights, which can only be found in a small group of IT specialists like administrators, architects, maintenance or computer security engineers.

Of course, insiders could be found in this population but real life has shown something very different.

By analyzing TTP’s (Tools, Techniques and Procedures) of cyber attacks, some use cases with insiders can be highlighted.

Indeed, cyber attacks on critical or high value network, which are more and more protected require alternative means to bypass defensive measures. For targeted attacks like Advanced Persistant Threat (APT), which are interactive and extend over a long period of time, a group of attackers will gain entry by any means in the network and from there, will discreetly study it, execute reconnaissance and adapt their attacking tools to gain better logical access until they reach their goal and strike.

The threat actor, when confronted with an air gap or a very well hardened network, will have difficulties to penetrate the outward perimeter, he will thus tend to use an insider to get first a physical access to the network, primarily to establish a covert communication channel (either through the Internet or by another means) with the main team waiting discreetly and anonymously outside the network. He will then proceed to the following steps of the attacks by escalating privilege and moving laterally, without the insider’s help.

In that case, the insider has just a very basic and one-time role to plug a device or execute a single action, the rest of the attack will be conducted from elsewhere thanks to the remote connection. In fact, he doesn’t need to know computer science or to have technical knowledge, he just needs to have a physical access to a network device.

In conclusion, insider threat covers a short but essential and critical phase in the overall computer attack and there is indeed no specific profile for insider in computer security.

We should consider two criterias when assessing this threat:
- Physical access to an element of the network with which an insider can interact. That could be an endpoint, switch, firewall... or a simple ethernet plug.
- Possibility of setting up a covert communication channel with the outside world. It should be noted that the second criteria is not necessary if the opponent has an exhaustive knowledge of the targeted system and is able to program an autonomous malicious code.
State
France

Gender
Male

Primary author: Mr FICHOT, Olivier (IRSN)
Presenter: Mr FICHOT, Olivier (IRSN)

Track Classification: CC: Information and computer security considerations for nuclear security
Implementation of the risk informed approach for the development of requirements to the physical protection of radioactive material and associated facilities

Radioactive sources and associated facilities are used in the world widely – in medicine, industry, agriculture, geological exploration etc. Depending on the type of their application, the characteristics of radioactive sources are also different - it could be a high activity radioactive source for radiotherapy treatment or a very low activity source in a chromatograph device. Conditions of the use of radioactive sources are specific either – an associated facility can be located in a populous district or in sparsely one, a number of people who can access to the radioactive sources are not fixed. Territorial location defines possible groups of potential adversaries that could be considered like the threat.

In accordance with the Essential element 9 "Use of risk informed approaches" from IAEA Nuclear Security Series publication No 20, all of these mentioned factors should be taken into account by a regulatory body when requirements to nuclear security systems and nuclear security measures for radioactive sources and associated facilities are established. But how the regulatory body can implement this Essential element in practice? The paper will provide an answer to this question based on the experience of Rostechnadzor - the Russian regulatory body for safety and security in the use of atomic energy.

Ensuring of the physical protection of radioactive material, radiation sources in the Russian Federation is an essential condition for their use established in the Federal law of the Russian Federation № 170-FZ dated November 21, 1995. Operation of storage facilities without compliance with requirements for their physical protection is also prohibited. Requirements for the physical protection of radioactive substances, radiation sources and storage facilities are established in Federal rules and regulations in the field of nuclear energy. As a regulatory body, Rostechnadzor, has developed of the Federal rules and regulations “Regulations on physical protection of radioactive substances, radiation sources and storage facilities” (NP-034-15) that provides requirements to the physical protection of radioactive sources and associated facilities.

In the paper the elements of the risk informed approach, that applied by Rostechnadzor, will be described: the graded approach for physical protection requirements based on “security levels” concept, defence in depth principle for different security layers, categorization of radioactive material and associated facilities for security purposes, use of an adversaries model (threat assessment concept) to define a set of adequate physical protection measures. The paper will also provide information about special approaches that were implemented to establish requirements to the physical protection of sealed radioactive sources categories 4 and 5, radioactive sources located at nuclear sites.

The paper and the presentation at the Conference will be of interest to representatives of regulatory bodies of IAEA Member States with responsibilities on the development of regulatory requirements to the physical protection of radioactive material and associated facilities, taking into account IAEA recommendations.

State

Russian Federation
Gender

Male

Primary author: Mr IVANOV, Maksim (Federal Environmental, Industrial and Nuclear Supervision Service of Russia)

Presenter: Mr IVANOV, Maksim (Federal Environmental, Industrial and Nuclear Supervision Service of Russia)

Track Classification: PP: Risk-informed approach to the security of radioactive material in use and in storage
The making of performance-based regulations

Canada is enhancing its Nuclear Security Regulations to be more performance-based. In removing prescriptive language from the regulations for a new performance-based one, the Canadian Nuclear Safety Commission (CNSC) needs to amend several key supporting documents, in particular the Design Basis Threat (DBT).

This paper will demonstrate the need for ensuring a collaborative approach across all areas of security, when developing modern regulations and regulatory documents that will provide expectations on how to nuclear facilities from evolving threats.

Addressing New Technology
How do we predict what security measures are needed when new technology is yet to be developed?
Several vendors have submitted proposed designs to the CNSC for review of potential small modular reactors. CNSC must clearly understand the technology, the categorization of nuclear material to be used, the use of the reactor, any waste produced by the reactor, and the site where this technology will be located. Regulatory requirements for protecting the nuclear material from theft and the facility from sabotage must incorporate a security risk assessment and security by design.

Incorporating Cyber Security
How do we capture cyber security requirements and incorporate them into regulations that are heavily based on physical security? Physical security specialists must work with systems engineering specialists to ensure that the DBT includes the various cyber threats that could impact the operations of a nuclear facility. New regulations must include input from cyber experts. Requirements for protection of nuclear facilities must incorporate computer security measures. Security evaluations must include a cyber Threat and Risk Assessment that will consider the risk of cyber-essential assets being compromised.

Analyzing Evolving Threats
How do we ensure that security requirements will be adequate to allow licensed nuclear facilities to protect against the Design Basis Threat? CNSC has taken a different approach to amending the existing DBT. Staff decided early on that a collaborative approach across all areas of security was needed. An 8-member project team was created to ensure a robust process is followed to reach a defendable product. Phase 1 – Analysis involves the collection of data. Phase 2 – Development is the review of data and intelligence analysis. Phase 3 – Consultation includes reaching out to licensees through a classified workshop. Phase 4 – Approval consists of presenting the new DBT to the Commission for publication.

State
Canada

Gender
Male

Primary author: Mr POIRIER, Yves (CNSC)
**Presenter:**  Mr POIRIER, Yves (CNSC)

**Track Classification:**  PP: Design basis threat and threat assessment: prevention and protection
Nuclear Forensics Bilateral Cooperation between Canada and the United States

Canada and the United States view nuclear forensics as an integral component of a State’s nuclear security architecture and an important capability for responding to events involving nuclear or radioactive material outside of regulatory control (MORC). Both countries maintain a robust system of nuclear material security, accountancy and control that is augmented by a wide range scientific and technical capabilities and infrastructure to support the nuclear forensics mission.

Through ongoing collaboration, Canada and the United States are working together to advance technical nuclear forensics in several key areas. These include radiochronometry, development and production of certified reference materials, stable isotope signatures, data analytics and concepts for national nuclear forensics libraries (NNFLs). Although each country has its own unique approach to the radioactive and nuclear material characterization, analysis and data assessment to support nuclear forensics investigations, technical exchanges have been mutually beneficial for advancing both programs. This is particularly important given the large shared border between Canada and the United States, and thus the possibility that an incident may involve both countries.

As a result of this collaboration, Canada and the United States have confidence in each other’s scientific and technical nuclear forensics data analysis and provenance assessment processes, thereby contributing to stronger cross-border nuclear security. Furthermore, Canada and the United States share common objectives in promoting and supporting nuclear forensics capacity building around the world through various multilateral organizations and initiatives. The bilateral collaboration between Canada and the United States has positioned both countries to effectively jointly engage the international nuclear forensics community of practice through the development and delivery of capacity building initiatives and products that ultimately seek to strengthen the security of nuclear materials worldwide.

This paper will present an overview of the collaborative activities between Canada and the United States aimed at advancing technical nuclear forensics, as well as the joint activities aimed at promoting and supporting nuclear forensics capacity building around the world through various multilateral organizations and initiatives.

State
Canada

Gender
Male

Primary author: Dr EL-JABY, Ali (Directorate of Security and Safeguards, Canadian Nuclear Safety Commission, Government of Canada)

Co-authors: Dr JONKMANS, Guy (Centre for Security Science, Defence Research and Development Canada, Government of Canada); Ms SEMBLAT, Nathalie (Weapons Threat Reduction Program, Global Affairs Canada); Dr LAMONT, Stephen (Los Alamos National Laboratory, U.S. Department of En-
nergy): Dr MARKS, Naomi (Lawrence Livermore National Laboratory, U.S. Department of Energy); Mr PAPPAS, Richard (U.S. National Nuclear Security Administration, U.S. Department of Energy)

**Presenters:** Dr EL-JABY, Ali (Directorate of Security and Safeguards, Canadian Nuclear Safety Commission, Government of Canada); Dr LAMONT, Stephen (Los Alamos National Laboratory, U.S. Department of Energy)

**Track Classification:** MORC: Nuclear forensics
A direct-AMS multi-isotope survey of uranium ore concentrates

Uranium ore concentrate (UOC) is an important nuclear material of interest for Canada. A large-scale analytical program is being led by the Directorate of Security and Safeguards (DSS) of the Canadian Nuclear Safety Commission (CNSC) to establish a reference dataset of UOCs that have passed through and/or that are currently under Canadian regulatory control. Isotopic ratios are among the signatures being captured under the reference dataset. Accelerator Mass Spectrometry (AMS) has been used for the measurement of \( \frac{236U}{238U} \) and an assessment of \( \frac{187Os}{188Os} \) in the trace levels of Os in UOC samples. Furthermore, since UOCs are typically concentrated in uranium to \( \approx 70\% \) by weight, a direct-AMS assay method is possible in which the samples can be measured without time-consuming chemical digestion and processing. Using this direct-AMS approach, several related ratios (\( \frac{231Pa}{238U} \), \( \frac{230Th}{238U} \), \( \frac{226Ra}{238U} \), \( \frac{187Os}{188Os} \)) were also assessed within the data acquisition sequence used for measuring the \( \frac{236U}{238U} \) ratios, and \( \frac{185Re}{187Re} \), \( \frac{187Re}{188Os} \), \( \frac{191Ir}{187Os} \) and \( \frac{193Ir}{187Os} \) in the sequence for the \( \frac{187Os}{188Os} \) ratios. Ratios of these isotope measurements are used to calculate the \( \frac{187Os}{188Os} \) ratio and elemental ratios of Re:Os:Ir in the UOC samples. These results can be displayed in a “bar-code” pattern to simplify UOC source identification. Unexpectedly large \( \frac{236U}{238U} \) ratios (approx. 10^{-7}) were found in several UOC samples. The \( \frac{187Os}{188Os} \) ratio was also shown, for the first time, to be a viable supplementary signature for the discrimination of UOCs. This direct-AMS method may have the potential to become an effective tool for nuclear forensics provenance assessment applications for UOCs.

This paper will provide an overview of the UOC AMS survey method and results, and will discuss technical considerations related to the need for a wider range of reference materials, further refinement of the sputter target preparation, as well as the Cs+ sputter ion source itself.

State

Canada

Gender

Not Specified

Primary author: Dr ZHAO, X.-L. (Department of Physics and A.E. Lalonde AMS Laboratory, University of Ottawa)

Co-authors: Dr FRANCISCO, B.B.A. (Department of Earth and Environmental Sciences and A.E. Lalonde AMS Laboratory); Dr KIESER, W.E. (Department of Physics and A.E. Lalonde AMS Laboratory); Dr CLARK, I.D. (Department of Earth and Environmental Sciences and A.E. Lalonde AMS Laboratory); Dr EL-JABY, Ali (Directorate of Security and Safeguards, Canadian Nuclear Safety Commission, Government of Canada)

Presenters: Dr ZHAO, X.-L. (Department of Physics and A.E. Lalonde AMS Laboratory, University of Ottawa); Dr KIESER, W.E. (Department of Physics and A.E. Lalonde AMS Laboratory)

Track Classification: MORC: Nuclear forensics
The Global Initiative to Combat Nuclear Terrorism
Nuclear Forensics Self-Assessment Tool

For the past two-and-a-half years, the Nuclear Forensics Working Group (NFWG) of the Global Initiative to Combat Nuclear Terrorism (GICNT) has worked on the development of the Nuclear Forensics Self-Assessment Tool (SAT). The SAT is designed to assist a national government structure an interagency dialogue to inventory and assess its national nuclear forensics capability. Its purpose is to ensure that a State considers key scientific and technical, operational and policy-related questions when collecting information when undertaking the self-assessment process. By using the SAT, it is anticipated that a State will gain a clearer sense of its nuclear forensics requirements and a better understanding of its scientific, technical, operational and policy gaps, and how these can be addressed as part of both a near- and long-term strategy.

The SAT is divided into three components: A. Identification of Nuclear Forensics Stakeholders; B. Collection of Information Related to Current Nuclear Forensics Capabilities; and C) Identification of Strengths and Gaps. Component B is further divided into four worksheets that facilitate the collection of information on the status of a State’s nuclear forensics-related policies and legal frameworks, protocols and procedures for material evidence management, scientific and technical analytical capabilities, and human resource development strategy. The SAT suggests steps a country may take following the completion of the self-assessment; however, it does not prescribe what a national nuclear forensics capability should like, nor does it provide a State with solutions on how to address identified gaps. This paper will provide an overview of the SAT and a detailed discussion of the worksheets in Component B. It will also discuss proposed strategies for facilitating the use of the SAT collecting information derived from its use.

State
Canada

Gender
Male

Primary authors: Dr EL-JABY, Ali (Directorate of Security and Safeguards, Canadian Nuclear Safety Commission, Government of Canada); Dr SCHNAARS, David (Office of the Under Secretary for Arms Control and International Security, U.S. Department of State)

Presenters: Dr EL-JABY, Ali (Directorate of Security and Safeguards, Canadian Nuclear Safety Commission, Government of Canada); Dr SCHNAARS, David (Office of the Under Secretary for Arms Control and International Security, U.S. Department of State)

Track Classification: MORC: Nuclear forensics
Advancements in Hardening the Cybersecurity Posture of Nuclear Power Plant Defense-in-Depth Network Architecture

Organizations increasingly depend upon cyber-based technologies for the reliable operation of Nuclear Power Plant (NPP) facilities through a myriad of Information Technology (IT) and Operational Technology (OT) systems. This enables the automation of industrial processes and a heightened exchange of information, however it also increases the attack surface which can be exploited by potential cyber-capable adversaries. To counter this, the International Atomic Energy Association (IAEA) proposes a defensive computer security architecture approach for strategically deploying computer networks as well as control systems through layers of securely defined levels and zones. To validate this type of architecture and to prepare for potential cyberattacks, Canadian Nuclear Laboratories (CNL) is actively performing research activities on numerous fronts. This paper will outline the advancements being made at the CNL’s National Innovation Centre for Cybersecurity in collaboration with the IAEA’s Coordinated Research Project (CRP) J02008, entitled ‘Enhancing Computer Security Incident Analysis and Response Planning at Nuclear Facilities’.

The foundation of CNL’s research in this area is a scaled down Boiler Level Control (BLC) system which integrates a software simulation of a Pressurized Water Reactor (PWR) in a feedback loop. With this experimental setup, cyberattacks can be conducted against the Programmable Logic Controllers (PLCs) managing the BLC and their supporting computing infrastructure, allowing the physical impact of cyberattacks to be measured in real-time. This segment of a NPP digital OT network is mission-critical for reliable NPP operations, and thus has significant measures in place to prevent malicious intrusion (e.g. unidirectional data diodes and no outside network connectivity). This segment is hardened but still vulnerable to insider threats, whether intentional or accidental, particularly as software changes and updates are introduced to the operational environment from engineering workstations. This paper will provide results on what type of cyberattack scenarios can affect this architectural segment, what organizational change management policies could be in place to prevent the delivery of a malicious payload, what are the symptoms of a cyberattack, and what actions could be taken in the event of a compromise.

The defensive computer security architecture paradigm puts a number of barriers in place across network segments, yet these measures may only delay a motivated Advanced Persistent Threat (APT) actor-group in a protracted cyber-intrusion campaign. Nevertheless, with enough of these obstacles to overcome, an attacker will likely leave some ‘footprints’ as they perform reconnaissance on the systems they are attempting to compromise. Anomaly detection tools provide a means to detect network traffic which is unaccounted for in an organization and can be used to detect an intruder. Commercial-off-the-shelf (COTS) anomaly detectors are made to be general purpose and it is unclear how they will perform in a NPP OT environment. CNL is also actively developing an anomaly detector to complement current COTS offerings. This paper will provide a benchmark of the techniques used within CNL’s anomaly detector against industry standard tools applied to a configuration resembling an NPP OT environment. This will further be explored in a discussion on how a portfolio of commercially available tools could be used to secure NPP networks in a connected IT-OT Security Operations Center (SOC).

In summary, the underlying goal of this paper is to share with the international community the advancements being made at CNL for ensuring a hardened defensive posture against NPP cyberattacks. The paper will provide a description of CNL’s NPP hardware-in-the-loop (HIL) architecture, an overview of its segmented computer network structure, results of penetration testing scenarios, benchmarking of custom anomaly detector tools against COTS technologies, design strategies for an IT-OT SOC, and recommendations for how an NPP organization could react in response to a cyber-intrusion.
**State**
Canada

**Gender**
Male

**Primary author:** Mr NEAL, Christopher (Canadian Nuclear Laboratories, Polytechnique Montréal)

**Co-authors:** Mr TRASK, David (Canadian Nuclear Laboratories); Mr DOUCET, Richard (Canadian Nuclear Laboratories); Mr THIYAGARAJAN, Karthik (Canadian Nuclear Laboratories); Mr ADAMSON, Peter (Canadian Nuclear Laboratories); Mr DALEY, Matthew (Canadian Nuclear Laboratories); Mr FERNANDEZ, José (Polytechnique Montréal)

**Presenter:** Mr NEAL, Christopher (Canadian Nuclear Laboratories, Polytechnique Montréal)

**Track Classification:** CC: Information and computer security considerations for nuclear security
Operating procedure for Radiological Crime Scene Management: harmonized on-site work between crime scene investigators and radiological experts

Terrorism is a growing trend nowadays. Radioactive materials can become explicit targets for crimes and for terrorist organizations, as they can be used in various weapons (such as explosives capable of dispersing radioactive material) resulting effective panic and serious economic damage.

Increasing terrorism serves growing chance to have different nuclear security events like radiological terror attack.

The severity of the problem is also illustrated by the fact that international organizations (such as the International Atomic Energy Agency, the Global Initiative to Combat Nuclear Terrorism, the Nuclear Forensics International Technical Working Group, ITWG, etc.) place great emphasis on this area. They seek to draw attention to the significance and dangers of the topic in major international forums (such as the Nuclear Security Summits).

Based on our experience, nuclear or other radioactive materials can be found at more and more crime scenes in Hungary. Already the recognition of these materials can be challenging in the absence of appropriate detection tools. Their precise identification, collection and professional transport, handling and examination require special expertise.

Particular attention needs to be paid to the fact that, in a crime scene, where appropriate, radioactive material may not be “uniform” (e.g. in closed packaging or in a container, box, sealed form), but may also be present as a contamination on various surfaces such as floor, wall, table tops, clothing, etc. Radioactivity is hardly detectable in the absence of appropriate measuring instruments. It also means that the radioactive material can contaminate the traditional evidences and response personnel like crime scene investigators.

Investigation of such a crime scene requires very special preparedness, rules and procedures. An important issue is the personal, health safety (radiation protection) of crime scene investigators and the special security and safety rules for collection, transport and subsequent investigation of radiological materials and radioactive contaminated traditional forensics evidences.

In most of the countries, including Hungary, there is a problem - which makes it difficult to develop effective procedures - that people who are responsible for (traditional) crime scene investigation are not prepared for the collection, handling and analysis of radiological materials (lack of expertise and equipment). While radiology experts (nuclear physicists, radiochemists) and their facilities − mostly research institutes - are not ready and allowed to collect, handle and investigate traditional forensics evidences: neither expertise nor permission.

Therefore, in Hungary we aimed to develop common standard operating procedures between radiological and traditional forensics experts for radiological crime scene management together with method developments for handling and analysis of radioactively contaminated traditional forensics evidences.

In the program traditional and nuclear forensics experts developed a procedure how to work together at a radiological crime scene and how to collect and investigate the evidences (radiological, traditional and radiologically contaminated traditional) in the field and examine at the laboratory in glove box. Research on the effects of the radiation on traditional evidences was also carried out. The method development was also focusing on safe conditions on evidence collection using special type of sampling kits and model contamination at a scene to test the safe collection.

This project was supported by the Hungarian Ministry of Interior in the frame of the Home Security Fund (BBA-3.3.3/3-2017-00010).
State

Hungary

Gender

Female

Primary authors:  Ms KOVACS-SZELES, Eva (Hungarian Academy of Sciences Centre for Energy Research); Ms CSOME, Csilla (Hungarian Academy of Sciences Centre for Energy Research); Mr TOBI, Csaba (Hungarian Academy of Sciences Centre for Energy Research); Mr ALMASI, Istvan (Hungarian Academy of Sciences Centre for Energy Research); Mr BODOR, Karoly (Hungarian Academy of Sciences Centre for Energy Research); Mr VOLGYESI, Peter (Hungarian Academy of Sciences Centre for Energy Research); Ms KAKUJA, Izabella (Hungarian Police National Bureau of Investigation Crime Scene Department); Mr BALASKO, Akos (Hungarian Police National Bureau of Investigation Crime Scene Department); Mr VOLARICS, Jozsef (Hungarian Police National Bureau of Investigation Crime Scene Department); Ms KREITZ, Zsuzsanna (Hungarian Police National Bureau of Investigation Crime Scene Department)

Presenter:  Ms KOVACS-SZELES, Eva (Hungarian Academy of Sciences Centre for Energy Research)

Track Classification:  MORC: Coordinated response to nuclear security events
Preventing illicit trafficking of nuclear and radioactive material

The aim of this synopsis is preventive action aimed at the identification of illegal transportation of radioactive material. It is to be expected that smugglers will avoid border crossings and checkpoints where radioactive radiation can be detected. This work aims to create additional devices that send the status of the Personal Radiation Detector (PRD) alarm via the mobile telephony network, such enabling remote monitoring of selected locations. PRD with additional devices should be hidden at toll booths, petrol stations, traffic lights, narrow roads which are used for illegal border crossings and other places that allow slow passage of the vehicle or its stopping near the hidden detection station. This enables continuous control of a large number of vehicles, such increasing the likelihood of detection of unauthorized transport of radioactive materials. The latest generation equipment manufacturers have no PRDs that can be connected to the network of the mobile operator. On the market, there are PRD’s of the latest generation that only have a bluetooth connection with a mobile phone and are designed for measurements from a distance of several meters. This paper aims to offer a technical solution in order to signal the status of the alarm sent through the network of the mobile operator. The PRD alarm signal is a light and vibration. As PRD is used as a hidden station, therefore, it is in a darkened area, the light of the display the alarm can be a trigger that will send an alert in the form of a call or SMS message to an already predefined phones whose number entered into the microcontroller.

The photo resistor is an electrical component that changes its resistance by changing the intensity of light. In this way, it is possible to detect the change of light, that is the status of the alarm on the PRD display. Vehicle identification is done by means of a camera or an existing video surveillance that is synchronized with the work of a hidden station for the measurement of radioactive radiation. Several stations on one section of the road can measure the radioactivity of almost every vehicle, with regard that the vehicle will be stopped at least one of several traffic lights.

It can also be used in conditions of illegal border roads. The system should be protected from low temperatures. Of course, this concept in one location should not have a high price, which allows covering a large number of potential illegal crossings. In these conditions, the autonomy of the work can be greatly increased, because the external batteries can be hidden, buried, which allows for a great autonomy of operation. The same system can be added to devices such as motion detectors, external cameras used by border police and hunters. Although the border can be very long, monitoring can be carried out successively. Information on threat assessments, ITDB and other information can be used in the preventive action against illegal international transit of nuclear and other radioactive material.

State
Montenegro

Gender
Male
Primary author: Mr PAVLICEVIC, Dragan (National Security Agency)
Presenter: Mr PAVLICEVIC, Dragan (National Security Agency)

Track Classification: MORC: Preventing illicit trafficking of nuclear and radioactive material
Experience in Chile, under National Coordination Mechanism for Emergency Preparedness and Response and the Prevention and Response for Nuclear Security Events

In Chile, the Commission on Safety and Security for Radiological Emergencies, CONSER, was created by Decree No. 647, in December 2015 with the mission of advice and support the Presidency of the Republic, in strengthening the capacity of prevention and reaction of the competent institutions to nuclear or radiological events, that may affect public security, safety of people or the environment.

In general terms, the functioning of the Commission has developed steadily, not being exempt from the difficulties inherent in a coordination mechanism, but important efforts are being made to fully develop the monthly meetings established and execute the planned activities, some of which are briefly delineated in this work. It should be noted that this coordination mechanism was informally generated in 2010, from a radiological emergency exercise organized by the Chilean Nuclear Energy Commission, CCHEN with support of the US-DOE.

From March 2016 to date, CCHEN has developed the activities assigned to the Executive Secretariat and organizing committee of the CONSER, which has generated a strong interface at national level in the preparation and response to radiological emergencies with the prevention and response to nuclear security events. Examples of strong interaction and permanent interfaces in these matters are the following:

a.- As of 2018, the CONSER Presidency mandated the Executive Secretariat to act as technical leader for the priority activity related to "Generation of National Emergency Plan for Radiological Risk Variable'. To date, May 2019, the work carried out is 70% complete, and it is expected to be finalized by end 2019, with a final review from an expert of the International Atomic Energy Agency, IAEA, within the framework of a on-going Technical Cooperation Project.

b.- Participation of most CONSER organizations in the activities organized by NSSC-CCHEN project under development. In 2018 a regional workshop was held on Creation of Regional Human Capacities in Nuclear Security, with the participation of representatives of Customs, Police and Regulatory Authorities of several countries of the region.

c.- CCHEN organized locally the workshop - mission to update the Integrated Nuclear Security Support Plan, INSSP, that was held in October 2018, with participation of 30 persons, members of 15 CONSER organizations. The mission resulted in the agreement for a new INSSP implementation plan 2019-2022.

d.- One of the permanent activities of CONSER is the periodic notification and updating of radiological incidents occurring at national level. This is generated from information arising from the two regulatory authorities and notified to all CONSER organizations. This activity has allowed the generation of a national statistics, a data base initiated on November 2013, which records the number of events, type of event, radioactive source or nuclear material involved, location, etc. This information is now expected to be analyzed in a systematic way to agree on national coordination activities aimed at minimizing its occurrence and facilitate its resolution.

e.- Representatives of CONSER organizations have participated periodically in training activities and expert missions in Preparedness and Response to Radiological Emergencies, carried out through one on-going IAEA TC project. Between 2016 and 2018, several activities of this type were conducted, covering topics related to first response, practical exercises, arrangements to protect the public in radiological accidents, generation and application of coordinated response protocols for the programmed transport of high-intensity radioactive sources among others.
In summary, it has been possible to combine and coordinate efforts of at least 18 national organizations that have functions and responsibilities at national level in the response to radiological emergencies in the country or at border points, and in the application of response protocols to events that affect public security, such as nuclear security events, the most common, the theft or missing of mobile radioactive sources, low intensity and low hazard, but of widespread use that causes increasing public concern.

Through the CONSER implementation, Chile has made progress in complying with the recommendations of the International Legal Framework in Nuclear Security and Emergency Preparedness and Response, regarding the establishment of a coordination mechanism among all national organizations involved in both fields, that in Chile are almost the same.

State
Chile

Gender
Female

Primary author: Ms VILLANUEVA-ZAMORA, Loreto (Chilean Nuclear Energy Commission, CCHEN)

Presenter: Ms VILLANUEVA-ZAMORA, Loreto (Chilean Nuclear Energy Commission, CCHEN)

Track Classification: CC: National nuclear security regulations
Experience Sharing from Nuclear Security Measures for 2018 PyeongChang Winter Olympic

The international & national efforts for reducing the threat of radiological terrorism and for responding to radiological emergency effectively have been strengthened. The organization of a major public event may give rise to security challenges and potential threats leading to health, social, psychological, economic, political and environmental consequences. The purpose of this paper is to introduce the implementation activities fulfilled for preparing 2018 PyeongChang Winter Olympic hosted by Korea and to share the experience and lessons learned. We fulfilled special inspection on high risk radioactive sources in advance to the Olympic. Also, we activated the emergency management system and dispatched the in-field response team and equipment to establish the defense-in-depth system for radiation detection, to enhance environment monitoring. As a result, there was no real event related to the radioactive material during the Olympic period. All of these endeavors contributed to most successful and safe Olympic. Korea will walk in step with international nuclear security regime consistently.

State
 Republic of Korea

Gender
 Male

Primary authors:  Mr KWON, Jeongwan (Korea Institute of Nuclear Safety); Dr PARK, Changsu (Korea Institute of Nuclear Safety); Dr YU, Hyungjoon (Korea Institute of Nuclear Safety); Mr CHOI, Changil (Korea Institute of Nuclear Safety); Mr LEE, Hyunseok (Korea Institute of Nuclear Safety); Mr LEE, Jeongtae (Korea Institute of Nuclear Safety)

Presenter: Mr KWON, Jeongwan (Korea Institute of Nuclear Safety)

Track Classification: MORC: Nuclear security as part of the security of major public events
Efforts on strengthening nuclear security from technology development perspective in JAEA

In 2010, the Japanese Government issued the national statement at Nuclear Security Summit (Washington D.C., USA) to develop technologies related to measurement and detection of nuclear materials and nuclear forensics, and to share them with the international community. In response to this statement, Integrated Support Center for Nuclear Nonproliferation and Nuclear Security (ISCN) was established in December 2010 in Japan Atomic Energy Agency (JAEA) which is Japan’s sole comprehensive research and development institute in the field of nuclear energy. ISCN has been carrying out R&Ds on innovative technology for measurement and detection of nuclear materials and nuclear forensics technical capabilities since Japanese Fiscal Year of 2011. This paper summarized the 10-year-efforts on technology development to strengthen nuclear security.

Non-destructive Assay (NDA) methods are an efficient and quick way for detection and quantification of nuclear materials. Main challenges to measure and detect nuclear material are to detect it hidden in heavy-shielded container and to measure it in high radiation environment and complex compositon. The passive NDA techniques are widly applied in nuclear filed, however they are not applicable to those conditions because emitted radiation is completely shielded and radiation background interfer target spectrum. Active NDA techniques utilize interrogation particles e.g. photons and neutrons inducing nuclear reactions to generate a radiation signature form a sample. Measurement and analysis of the induced differences in radiations and incident particles are used to extract information of nuclear and matrix materials in the sample. These methods are potentially applicable to analysis of high-level radioactive nuclear materials and to detection of nuclear materials in a heavy shield. One of the programs to develop active NDA technique is “Development of Nuclear Resonance Fluorescence (NRF) technique” for detection of nuclear materials hidden in heavy-shielded container. This technique utilizes quasi monochromatic gamma-ray beams produced by laser Compton scattering (LCS). The energy of LCS gamma-rays is tuned to a nuclear resonance energy of a nuclide to be found. NRF gamma-rays induced by LCS gamma-rays are observed by gamma-ray detectors. The first part of this program carried out technological development on high-intensity quasi-monochromatic LCS gamma-ray beam production, and then an experiment using an NRF NDA technique will be performed to demonstrate nuclear material detection hidden in a heavy shield in March 2020. Another program is “development of active neutron NDA techniques”, in which four techniques are developed in an integrated manner, i.e. Differential Die Away Analysis (DDA), Delayed Gamma-ray Analysis (DGA), Neutron Resonance Transmission Analysis (NRTA), and Prompt Gamma-ray Analysis (PGA). These techniques could be used to complement each other and would be applicable to nuclear security purposes for detection of nuclear material and explosive materials as well as nuclear material accountancy for both low and high level radioactive sample. Basic development of four techniques were carried out and the phase-2 for focusing analysis of high level radioactive sample is currently under way.

Since initiation of nuclear forensics technology development, the fundamental nuclear forensics analytical capabilities were established for characterization of nuclear materials and prototype nuclear forensics library for interpretation of the analytical results in first three years. ISCN has also engaged in development of advanced technologies for more rapid and precise nuclear forensics analysis and shared the achievements for strengthening international nuclear forensics capabilities. It includes new uranium age dating methods, data analysis methodology for library based on multivariate analysis and image analysis methodology for particle characterization. These technical capabilities have been validated through the joint research with the U.S. national laboratories and Europium Commission Joint Research Center (EC-JRC), and participation in exercises organized by International Technical Working Group. In order to sustain and improve the capability, new technical efforts were recently initiated. The development of post-dispersion event technology covers supporting for detection and recovery of radioactive samples from an event scene, and measurement and signature analysis methodology for post-dispersion samples. As the innovative
technology, machine-learning algorithm for data analysis on nuclear forensics library, and application of autoradiography for nuclear forensics purpose are being studied. In order to identify the technical needs to be developed and share our achievements to both domestic and international stakeholders, the international technical symposiums and workshops were held. Each R&D program was basically conducted for three to five-year basis and was evaluated by international experts at the end of program and the feedback applied to next program. The identified needs from domestic and international community reflect subjects of future program. These communication with stakeholders could also be contributed filling the gap between R&D achievement and implementation in real field, which is one of the most difficult challenges.

The R&D programs on contributing nuclear security in JAEA are being conducted by subsidiarly budget for nuclear security promotion of the Ministry of Education, Culture, Sports, Science and Technology of Japan through collaboration with U.S. Department of Energy and EC-JRC, and Japanese institutes and universities.

State
Japan

Gender
Not Specified

Primary authors: TOMIKAWA, HIROFUMI (Japan Atomic Energy Agency); KOIZUMI, Mitsuo (Japan Atomic Energy Agency); KIMURA, Yoshiki (Japan Atomic Energy Agency); OKUBO, Ayako (Japan Atomic Energy Agency); HORI, Masato (JAEA); NAOI, Yosuke (Deputy Director, Integrated Support Center for Nuclear Nonproliferation and Nuclear Security, JAEA)

Presenter: TOMIKAWA, HIROFUMI (Japan Atomic Energy Agency)

Track Classification: CC: Advances in nuclear security research and development; international cooperation on nuclear security research
LESSON LEARNED FROM NUCLEAR SECURITY SYSTEM AND MEASURES OF THE MAJOR PUBLIC EVENT (MPE) IN INDONESIA: THE PREPARATION, IMPLEMENTATION, AND ROLE OF INTERNATIONAL SUPPORT

ABSTRACT

LESSON LEARNED FROM NUCLEAR SECURITY SYSTEM AND MEASURES OF THE MAJOR PUBLIC EVENT (MPE) IN INDONESIA: THE PREPARATION, IMPLEMENTATION, AND ROLE OF INTERNATIONAL SUPPORT

Indah Annisa (i.annisa@bapeten.go.id)
Head of Cooperation Division, BAPETEN

Nuclear security is the prevention and detection of and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities and activities. In 2018, Indonesia were hosting 2 (two) grand and important event: The 18th Asian Games, and The IMF and World Bank Annual Meeting. The 18th Asian Games 2018 is a quadrennial sport event in which involving athletes from countries in Asia region, whilst the IMF and World Bank Annual Meeting brought together all state top leaders, ministers, central bankers, and many important figures in finance industries. These both events are categorized as Major Public Event (MPE). MPE is a huge planned event at national or international level in which involving a large number of resources and requires good planning and the implementation of a maximum security plan. In this case, nuclear security issues become very essential considering various credible threats, for instance criminal act or terrorism involving nuclear material or other radioactive sources, either in the form of Dirty Bomb/Radiological Dispersal Device (RDD), as well as Radiological Exposure Device (RED). This paper aims to identify lesson learned from nuclear security system and measures in the preparation, implementation, as well as support from international organization or partners, particularly from the IAEA. In the stage of preparation, coordination with relevant security agencies and stakeholder institutions became essential factor to establish a good national strategy for planning, preparedness and implementation of nuclear security system and measures. Several meetings and coordination with parties involved in the events have been conducted, as well as facilitated many workshops to enhance the human resources capabilities of our security agencies and institutions with the support of international partners. During the implementation, we conducted mapping for background radiation in venues and strategic locations, screening, monitoring, and response. We received assistance from the IAEA for radiation detection equipment a number of 100 PRD (Personal radiation detector), 10 RID (Radioactive Identifier Device), and 8 PRS (Portable Radiation Scanners). This assistance from the IAEA was one of the action plan agreed in the INSSP. Both events were held successfully, there were no significant security problems. However the procedures should be better prepared and well coordinated in advance. Appreciation came from the Government of Indonesia as well as from participating countries.

Keywords: nuclear security system and measures, MPE, international support

State
Indonesia

Gender
Female

**Primary author:** ANNISA, Indah (Nuclear Energy Regulatory Agency of Indonesia (BAETEN))

**Presenter:** ANNISA, Indah (Nuclear Energy Regulatory Agency of Indonesia (BAETEN))

**Track Classification:** MORC: Nuclear security as part of the security of major public events
Myanmar’s Effort to Sustain National Nuclear Security Regime and International Cooperation in Strengthening of Nuclear Security

Myanmar, a State with very limited quantities of nuclear material, acceded to the Convention on the Physical Protection of Nuclear Material (CPPNM) and its amendment on 6th December 2016 and entered into force on 5th Jan 2017. Following the accession to CPPNM and its amendment, Myanmar is working step by step approach to implement the obligations under the convention.

The utilization of radiation sources is limited to the use in medicine, industry, agriculture, livestock breeding and research. To promote the protection of radioactive material in use, transport and storage and to establish the security detection architecture for nuclear and other radioactive material out of regulatory control by international cooperation and domestic interfaces are further steps in the implementation of effective national nuclear security regime.

With the purpose of strengthening national nuclear related legislation, Division of Atomic Energy (DAE) under the Ministry of Education (MOE), has just recently completed the drafting of Myanmar Nuclear Law that prohibits the use, production, storage, distribution and import/export of nuclear and other radioactive materials without government license. Furthermore, Myanmar has expressed a political commitment with regards to the Code of Conduct on Safety and Security of Radioactive Sources.

The development of a number of regulations namely Nuclear Safety Regulation, Nuclear Security Regulation and Safeguards Regulation will follow. Counter Terrorism Law Myanmar was promulgated on 4th June 2014, and it is based on UNSCR 1373 and UNSCR 1540 which is related to nuclear security issues. The DAE acts as the Regulatory Body under the Atomic Energy Law and is responsible for all aspects of control, security and safe management of radioactive materials used in Myanmar.

The DAE is using Regulatory Authority Information System (RAIS) since 1998 and now using RAIS 3.3. The DAE collect the list of the private clinics, hospitals, industries with their radioactive source and radiation apparatus by the help of relevant Ministries. The Inspectors from DAE also disseminate security culture for radioactive sources to pave way for future use of Nuclear Security practices among private and government sectors.

Establishment of recording and reporting of incidents to regulatory authorities will come soon. Reporting systems for medical radiation incidents become Mandatory reporting as part of regulation. All detected event are notified initially to the IAEA Incident and Trafficking Database (ITDB).

For international cooperation, DAE has been engaging Integrated Nuclear Security Support Plan (INSSP) and Global Threat Reduction Initiative (GTRI) programme, in collaboration with International Atomic Energy Agency (IAEA), United States Department of Energy (USDOE), Australia’s Nuclear Science and Technology Organisation (ANSTO) , Korea Institute of Nuclear Nonproliferation and Control (KINAC) and ASEAN Centre for Energy (ACE). Moreover, regarding with strategic trade control and container control, Myanmar cooperates with Australian Border Force (ABF), United Nations Interregional Crime and Justice Research Institute (UNICRI) and the European Union Chemical Biological Radiological and Nuclear Risk Mitigation Centres of Excellence Initiative (EU-CBRN COE), in conjunction with local stakeholders.

Myanmar, in collaboration with the IAEA and USDOE, is now endeavoring to implement the physical protection systems at the Radiotherapy Departments in the Government Hospitals and recently established Central Monitoring Station in the DAE branch office in Yangon.

DAE hosted a team from USDOE, National Security Administration’s Office of Radiological Security (ORS) for Site Assessment Visit from 13 to 23 May 2019. Expert team from USDOE visited...
Mandalay General Hospital and inspected the installations of physical protection systems to secure the Co-60 teletherapy unit, then visited Taunggyi Saq San Tun General Hospital to make design calculations for coming installation.

Moreover, this expert team conducted International Response Training in Nay Pyi Taw. Training is designed to assist partner countries with establishing and maintaining effective response capabilities in the event of an attempted theft of radiological material. It helps the relevant ministries in Myanmar to understand the threats and plan to respond for radiological security incidents.

The DAE raises awareness to maintain and further strengthen national nuclear security regimes in strengthening nuclear security globally through Media and social network for public awareness, engagement in national and international events, and translation of technical document into the national language and sharing of information and good practices with relevant stakeholders.

Radiation Protection Training for radiographers from Medical field is being conducted each year. Outreach disseminations of CBRN are conducting for Law Enforcement Departments each year and on demand. To enhance security in local and border areas, DAE is trying to get installation of radiation portal monitors.

This paper will highlight Myanmar’s consolidated efforts to sustain and further strengthen national nuclear security regime with special focus on nuclear security and radioactive source security still strives for continuous improvements to its performance of the control of radioactive material under and out of regulatory control and engagement with international organizations and domestic interfaces while preventing illicit trafficking of nuclear and radioactive material.

**State**

Myanmar

**Gender**

Female

**Primary authors:** Dr TUN, KHIN PA PA (Division of Atomic Energy, Ministry of Education); Dr AUNG MIN PHO SAW (Division of Atomic Energy, Ministry of Education)

**Presenter:** Dr TUN, KHIN PA PA (Division of Atomic Energy, Ministry of Education)

**Track Classification:** CC: Implementation of national legislative and regulatory frameworks, and international instruments
CHALLENGES FOR PHYSICAL PROTECTION OF INDONESIA EXPERIMENTAL POWER REACTOR

Currently Indonesia are expecting to build its first Experimental Power Reactor which has HTGR technology. The fuel design of the reactor will have the same type of fuel with HTR-10, a 10 MWt reactor in China. The fuel design of the reactor is pebble bed where the fuel is a collection of nuclear material inserted in small sized spheres containing structural and moderating material and a pebble bed core that will contain a bulk load of 27,000 spherical fuel elements. The refuelling scheme will use continuous multi-pass cycle where each pebble fuel will go through 5 operation cycles before taken out of the core as a spent fuel. Hence, these fuel design and fuel cycle management will provide different security challenges than the implementation in the common existing reactors. Modularity and size of the reactor which will be a small modular type of reactor will also have impact on the implemented physical protection. The implementation of Security-by-Design as the design progresses provides an approach to meets the security requirements needed.

State

Indonesia

Gender

Male

Primary authors: Mr NUGROHO, Tino Sawaldi Adi (Indonesia Nuclear Energy Regulatory Agency); Mr RUSMANATMOJO, Imron Tarsono (Indonesia Nuclear Energy Regulatory Agency); YULIATI, Evin (Bapeten)

Presenter: Mr NUGROHO, Tino Sawaldi Adi (Indonesia Nuclear Energy Regulatory Agency)

Track Classification: PP: Nuclear security of new nuclear technologies (e.g., small modular reactors)
Overview of strengthening the Nuclear Security Regimes for the Ghana Research Reactor-1 by the Ghana Atomic Energy Commission

The International Atomic Energy Agency (IAEA) through its publications had emphasised that the responsibility of nuclear security within a state rest entirely with the state in ensuring security of nuclear materials and other radioactive materials. In that regard, owners of nuclear facilities owns the state the responsibility of protecting such materials against theft, sabotage, unauthorized access and illegal transfer and other malicious acts. It is in this recognition that the Ghana Atomic Energy Commission (GAEC), owners of Ghana Research Reactor-1 (GHARR-1) over the years have been engaging the necessary international strategies in improving matters of nuclear security at the facility level.

GAEC was established by an Act of Parliament (Act 204) in 1965 with the mandate to be the sole authority in Ghana responsible for matters relating to peaceful uses of atomic energy and fulfilling the state’s obligation on nuclear safety and security. For the purpose of nuclear regulation, it established the Radiation Protection Board (RPB) by Atomic Energy Amendment Law (PNDCL 308) in 1993 as a national nuclear regulatory authority. The PNDCL 308 Law prescribe powers and functions of the RPB which include mechanisms for the safety and security of nuclear and other radioactive materials. To further improve the regulatory system in Ghana, the RPB was modified into an independent Nuclear Regulatory Authority (NRA) by Act 895 of Parliament in 2015. Act 895 empowered NRA to conduct inspections to assess compliance with the security of nuclear and radioactive materials and associated facilities. These arrangements have strengthened the effectiveness in the nuclear security regulatory regimes in Ghana as the NRA is currently drafting the national legislations in that regard.

Guided by these regulatory processes, GAEC acquired GHARR-1 which is a 30-kW commercial version of the Chinese Miniature Neutron Source Reactor (MNSR) and belongs to the class of tank-in-pool type reactors in 1994. The core of GHARR-1 which was initially 90.2% uranium enriched is located 4.7 m under water close to the bottom of a watertight reactor vessel. The quantity of water in the vessel, serves the purpose of radiation shielding, moderation and as well as primary heat transfer medium. Currently, the high enriched core of GHARR-1 has been converted to 13% low uranium enriched fuel in 2017. By the core conversion, GAEC has showed a strong commitment in addressing global matters of non-proliferation concerns and also strengthening its nuclear security regimes at the facility level. The commitment to non-proliferation dates back to 1968 as GAEC signed the safeguards agreement in 1975, and the Additional Protocol Agreement in 2004. For the commission to understand, gained international recognition and appreciate better matters of nuclear security at the facility level, over the years, has signed numerous international legal instruments which include: Convention on the Physical Protection of Nuclear Material (CPPNM); and Convention on Nuclear Safety (CNS). For the prevention of malicious acts by an adversary that could result in unacceptable radiological consequences, GAEC has in place a credible strategy which include: Physical protection, personnel security and emergency response plan to deal with such matters. Currently, the major security upgrades at GHARR-1 is based on three main basic physical protection systems of Prevention, Detection and Response.

Physical Barriers include: making the reactor hall resistant to force attack; outer border of the protected area has outside walls, bars on the glass windows, locked doors and locked gate; an access control turnstile is installed in the corridor leading to the reactor hall; a well-designed intruder detection system such as alarm sensor on the door, vibration sensors on the walls and
detection sensors on top of the reactor are installed at GHARR-1 to provide early and reliable
detection of any attempted intrusion; to improve verification capabilities, CCTV cameras or video
motion detection to monitor the internal areas of the reactor hall, control room and the reactor
hall corridor had been installed, the video data is stored and can always be played back. These
systems are connected to the central alarm station (CAS) and monitored externally 2 km at GAEC
police station which give signal of protected area violation by potential intruder. In addition, fresh
fuel is located at high security area physically separated from the fuel in the reactor core.
Personnel security arrangements are in place at the facility to ensure honesty, reliability and trust
worthiness of staff and others who have access to the facility. The objective of personnel security
is to ensure unauthorized removal and sabotage in the facility regarding nuclear and radioactive
materials. An emergency plan with an objective to effectively recover or mitigate consequences of
sabotage is well documented in the GHARR-1 Safety Analysis Report. Finally, GAEC with support
US Office of Radiological Security (ORS) is in the process of implementing a “Site Security Plan”
to boost security at its nuclear facilities.

State
Ghana

Gender
Male

Primary author: Dr ADDO, Moses Ankamah (Ghana Atomic Energy Commission)
Presenter: Dr ADDO, Moses Ankamah (Ghana Atomic Energy Commission)

Track Classification: PP: Research reactor security
Impact assessment of nuclear security events using chemical explosives

It has become easier for terrorists to obtain chemical explosives in recent years, with the spread of the internet. Also, examples of terrorism at nuclear facilities have been reported around the world. Hence, various measures against terrorism targeting nuclear facilities with chemical explosives have been implemented in many countries. On the other hand, that fact indicates the need of consideration that terrorists steal nuclear and/or radioactive materials and attach chemical explosives to them to increase the scale of the damage, taking large-scale events such as the Olympic Games into account. That is to say, the necessity of the post-dispersion study. In those nuclear security events, it would be assumed that the explosion by chemical explosives destroys objects containing the nuclear and radiological materials, and their debris containing those materials scatters around. Since these debris are radioactive, it is thought that evaluating the scattering behavior of the debris is useful in the radiation exposure evaluation of surrounding environment.

The United States and Japan established a bilateral Nuclear Security Working Group (NSWG) to strengthen nuclear security worldwide. One of the goals that the group developed was Goal 9 “Joint Study on Management of HEU and Plutonium: Reduction of Material Attractiveness,” which establishes through science-based study, a mutual understanding of the risk from non-state actors conducting malicious acts involving nuclear material and facilities. Eventually, the study evaluates the number of deaths, number of injuries, and the economic impacts when nuclear security events occur, in order to consider overall consequences. Therefore, the data of such scattering behavior would be useful. However, such research has not been done or has not been published to date.

ISCN under the JAEA is developing nuclear security technologies by utilizing JAEA’s knowledge, experience and technical capabilities in order to contribute to the peaceful use of nuclear energy. Based on the usefulness of the nuclear material scattering behavior mentioned above, ISCN analyzes the explosion and impact behavior of nuclear material in various forms by chemical explosives by simulation using ANSYS AUTODYN. The forms of nuclear material currently in the project scope are metals, oxides, powders and liquids. A benchmark experiment related to this is also planned. The application of the study would be to do the dose evaluation from scattered debris and create a map that shows the range of lethal dose, which possibly contributes for the Goal 9 study. In addition, based on such maps, it is possible to contribute to create an effective mitigation plan by response unit.

This work is supported by the Japanese Ministry of Education, Culture, Sports, Science, and Technology (MEXT) under the subsidy for the “promotion of strengthening nuclear security and the like.”
Presenter: SHIBA, TOMOOKI (Integrated Support Center for Nuclear Nonproliferation and Nuclear Security, Japan Atomic Energy Agency)

Track Classification: MORC: Coordinated response to nuclear security events
Identification of RBMK and VVER spent nuclear fuel batches by means of HGRS in course of forensic examination

This paper gives a study of the high resolutions γ ray spectrometry (HRGS) capabilities to define seized spent nuclear fuel (SNF) origin during its forensic examination in the first 24 hours of investigation. Keeping in mind the multicomponent nature of the spent nuclear fuel, during test method development attention was paid on the following set of nuclides: cesium-134, cesium-137, ruthenium-106, cerium-144, antinomy-125, europium-154, europium-155, uranium, plutonium, americium and curium.

With this purpose, a detailed gamma-spectrometric study of different VVER and RBMK SNF samples was carried out. Spectral analyses of these samples were made by means of two different instruments: HPGe planar photon detector system GLP-36360/13P4 and coaxial one GEM35P4-76. One of the greatest problems in SNF spectral analysis by means of HRGS is a continuous background signal in wide area of the spectra which is induced by γ-ray emission of fission products (first of all 137Cs). In the course of this study was found that HPGe planar detector is better for the task on hands then coaxial one. It is due to the difference of their intrinsic efficiency curves. It was found that U or Pu γ-ray emission signal can be reliably detected if 137Cs signal intensity is not more than ~600 times greater. This estimation has been made for HRGS spectral data with statistical uncertainty per channel below 3%.

According to calculated relative γ-emission intensities almost all γ-spectral lines of actinides in spectra of normal SNF batches are completely suppressed by background γ-emission of fission products or by spectral interferences. The same situation remains even after long cooling period of 30 years and more. There are only a few exceptions: 241Am, 243Am and 243Cm. Unfortunately, measured (current) activities of 241Am, 243Am and 243Cm are hard to use for SNF identification. In real practice 241Am presence in γ spectrum is good enough only for confirmation of seized sample’s nature as SNF. If SNF cooling period is known an up-to-date decay adjusted 137Cs/243Am activity ratio can be used to evaluate SNF burn-up. A very promising fingerprint signature of very high burn-up SNF batches is a 137Cs/243Cm activity ratio. The main advantage of this ratio is that it is almost independent towards SNF cooling period. It is because half-life periods of these nuclides are very close to each other and after longest possible SNF cooling period of about 60 years this ratio shifts only for ~5%.

Another case is a sample of abnormal SNF batch, which accidentally undergo partial separation of actinides and fission products. Uranium and plutonium nuclide γ-ray signals can be directly detected and measured in γ-spectra of such samples without any sample preparation. Abnormal SNF batches has a great significance as potential objects of forensic examinations, because during INES 6 and INES 7 class incidents many fragments of these batches can become out of regulatory control. In the present study γ-spectra of such abnormal SNF batches was obtained and successfully used to determine their 232U/235U isotope ratios.

In case of SNF the majority of γ-ray emission comes from γ-emitting fission prod-ucts that can be also referred as radionuclide markers. These radionuclides can be used itself to determine origin of seized SNF sample. In the present study activities of the following nuclides were measured in SNF samples: 125Sb, 134Cs, 137Cs, 154Eu and 155Eu. Activity ratios of these nuclides can be used as fingerprint signatures. Among all of these ratios the most useful one for SNF batch identification is a 137Cs/134Cs activity ratio. There is a common practice to measure this ratio for every SNF batch after the end of its irradiation to evaluate fuel burn-up value. Due to this practice, initial
value of this ratio is known for every SNF batch. So, this value can be taken from nuclear power plant archival records, up-to-date decay adjusted and used as a perfect fingerprint signature to identify seized SNF sample’s origin. If current measured value of seized sample’s $^{137}\text{Cs}/^{134}\text{Cs}$ ratio is equal to corresponding up-to-date decay adjusted initial ratio of some SNF batch it can be stated, that this batch is an origin of seized sample. Unfortunately, this method cannot be applied to other activity ratios of mentioned above radionuclides because there is no common practice to measure their initial activity ratios for every SNF batch after the end of its irradiation.

In conclusion of the IAEA project No18989 a test method for RBMK and VVER SNF identification by means of HGRS was developed and proposed. This test method could serve as a guideline for HGRS composition analysis and data interpretation in case of nuclear forensic examination of seized spent nuclear fuel samples.

State

Russian Federation

Gender

Primary authors:  Ms ANDREEVA, Alesia (Khlopin Radium Institute); Dr DUSHIN, Victor (Khlopin Radium Institute); Dr KRAMCHANINIV, Aleksey (Khlopin Radium Institute)

Presenter:  Ms ANDREEVA, Alesia (Khlopin Radium Institute)

Track Classification:  MORC: Nuclear forensics
Management of nuclear security-safety interface: what, why and how

What is safety-security interface and interface management

Security-safety interface is a decision point where both safety and security issues should be taken into consideration. When done in a risk-informed, balanced manner, this should result in best possible overall safety and security. Doing this—by effective processes and procedures—is safety-security interface management.

Interface management takes place at the government level: coordination between authorities, licensing, regulatory requirements, inspection programmes, and at the licensee level: primary responsibility of safety and security and implementation of regulatory requirements. In detection of and response to material out of regulatory control interface management enables efficient and secure communications, and fits together radiation safety and forensics procedures in crime scene management.

We endeavour to manage the safety-security interfaces in order to take advantage of synergies and to resolve possible conflicts.

Joint fundamental objective and difference

It is widely recognized that nuclear safety and nuclear security share a joint fundamental objective to protect people and the environment from harmful effects of ionizing radiation. If we consider that nuclear safety measures aim to ensure the safety of normal operations, a low probability of accidents, and effective emergency preparedness, and that nuclear security measures aim to combat intentional unauthorized acts, we can see that they approach their joint objective with different risk assessments and that both are equally necessary to achieve the overall objective.

The big difference is the “opponent”. Safety measures are designed against unintentional events. Security measures are designed to deal with active adversaries, who may adapt their actions based on their knowledge of the defences. In accident management it is good that procedures are widely known and that controls are easily accessible—in a security event the adversary would use that information and access to defeat the response.

Similarities and differences in practice

Many safety and security measures contribute to both regimes and complement one another. There is also potential for conflict.

Complementing elements include:

- Coordinated legal and regulatory framework
- Risk-informed, graded approach
- Safety and security by design of systems, structures, and components
- Integrated management system
- Human factors
- Organisational culture
- Information and computer security
- Access control and surveillance
- Materials accountancy
• Coordinated response

Potentially conflicting elements include:

• Transparency vs. confidentiality
• Control and delay of access & exit vs. unobstructed passage

There are also neutral elements that do not particularly contribute to or interfere with the other regime.

Some areas where interdependencies between safety and security are strong

Leadership, management and organizational culture

How nuclear safety and security are addressed in the integrated management system of an organization, is a top level interface management decision. Risk management is an example of a cross-cutting process where balanced approach to security, safety, and other risks should serve informed decision making. People should recognize the decision points where safety and security considerations matter.

Information and computer security

Information security—confidentiality, integrity and availability of information—links safety and security together in a concrete way: to ensure the information is accurate and complete, at the disposal of the right people at the right time, and not at the disposal of the wrong people. All three are essential for safe and secure use of nuclear energy and use of radiation in health care, industry and research as well as for effective response to accidents and security events, including MORC incidents.

The interdependence between computer security, physical security, and safety has grown in importance due to the increased use of digital, programmable, and networked systems, in OT as in IT.

Design and change management

The most efficient life cycle phase to pursue safety and security is the design. Industrial control systems should also have “hard-to-hack” as a design paradigm. Along the life cycles there are modifications. There should be steps in the procedures to flag safety-security decision points and who should participate in decision making.

Response

Response to anomalies is a test for safety-security interface management. The following activities should be implemented in a coordinated manner:

• accident/emergency response and nuclear security response
• on-site response and off-site response
• activities of all entities responsible for off-site response
• emergency exercises, security event exercises, and combinations thereof, including cyber and physical threats.

Some potential for further work

Classical safety classification of systems, structures and components does not necessarily account for intentional unauthorized acts. On the other hand, a balance should be found between security controls and usability. A holistic risk-informed approach for significance evaluation might be a good basis for further development.

Methods for application of probabilistic risk assessment (PRA) in security analyses and design have been and are being developed. The aim need not be to produce absolute values of risk, but,
for example, to compare the effectiveness of different nuclear security systems, and to balance safety and security aspects in the assessment.

State

Finland

Gender

Female

Primary author:  KARHU, Paula (Radiation and Nuclear Safety Authority (STUK))

Co-authors:  STAUFFER, Bernard (Swiss Federal Nuclear Safety Inspectorate (ENSI)); SCHRAVER, Marco (Authority for Nuclear Safety and Radiation Protection (ANVS)); HACK, Tapani (Radiation and Nuclear Safety Authority (STUK))

Presenter:  KARHU, Paula (Radiation and Nuclear Safety Authority (STUK))

Track Classification:  CC: Nuclear safety and security interfaces
IAEA Member States dedicate significant resources and effort to develop and implement their national nuclear security regimes, which are based on the capabilities to prevent, detect and respond to criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities, or associated activities. However, multiple examples and experience in member states has shown that the actions needed to sustain (ability to remain effective over the long-term) these capabilities require a systematic and consistent approach, government and competent authorities’ commitment and certain infrastructure. This is also comprehensively reflected in IAEA Nuclear Security Series No. 30-G "Sustaining a Nuclear Security Regime."

Based on member states requests for IAEA support in developing, implementing, and sustaining an effective national nuclear security regime and drawing from the experience of certain states, the IAEA developed a concept for the establishment and operation of a national Nuclear Security Support Centre (NSSC) as a means to strengthen the sustainability of nuclear security in a state. The concept was captured in the IAEA TECDOC 1734, "Establishing a National Nuclear Security Support Centre." As interest in the NSSC concept increased, the IAEA established the International Network for Nuclear Security Training and Support Centres (NSSC Network) in 2012 to facilitate sharing of information and resources and to promote coordination and collaboration among states with an NSSC or those having an interest in developing a centre.

The NSSC Network grew rapidly in its first few years, from 20 Member States in 2012 to 49 Member States by 2015. The growth in membership also reflected a wide range of NSSCs with diverse organizational structures, affiliations, objectives, and a variety of operational practices and approaches. However, after a few years of operation, the NSSC Network Members and the IAEA identified certain gaps and areas for improvement. In particular, the NSSC Network still had minimal understanding of NSSC needs and resources, insufficient data gathering and information management tools, a need for more strategic direction and agreed priorities within the Network, and a lack of detailed guidance and information on best practices for NSSCs.

This paper will outline the key actions that the NSSC Network has taken since 2016 in order to make it more effective. Significant achievements in that regard include: holding the NSSC Network Annual Meeting in Pakistan (2016), Japan (2018), and China (2019); developing a new NSSC Network database, events calendar, and semi-annual Newsletter; revising IAEA TECDOC 1734 to serve as enhanced guidance for States on establishment and operation of an NSSC; optimizing the schedule and content of Network meetings; developing a new long-term strategy for the Network; and revising and adopting a new Terms of Reference.

Implementing these key steps has helped grow the NSSC Network further to 61 Member States, and has enabled the IAEA and others to provide support for Members that is more structured, systematic, effective and efficient. The NSSC Network experience could therefore be a useful reference for other frameworks or initiatives for cooperation in nuclear security. Learning from the thoughtful approach to programme development within the NSSC Network could help other similar frameworks to avoid mistakes and achieve more consistent implementation of their objectives.
Lithuania

Gender

Male

Primary author: Mr LIVSIC, Aleksejus (Lithuanian Nuclear Security Centre of Excellence)

Co-author: Mr HAQ, INAMUL (PAKISTAN INSTITUTE OF ENGINEERING AND APPLIED SCIENCES (PIEAS))

Presenters: Mr LIVSIC, Aleksejus (Lithuanian Nuclear Security Centre of Excellence); CONNER, James (IAEA)

Track Classification: CC: Role of Nuclear Security Support Centers to support and sustain national nuclear security regimes
State-of-the-science atmospheric dispersion and source reconstruction modelling applied to the nuclear security

Nuclear and/or radioactive materials may present a serious health risk for the population when disseminated into the atmosphere (or as liquid effluents) or present as irradiating sources. The exposure of human beings to these materials can occur in various circumstances ranging from more or less serious accidents to criminal activities. Let it be of uncontrolled or of deliberate origin, events such as the dispersion of radionuclides or the existence of hidden / lost sources may be anticipated to potentially result in adverse human consequences and social disruption.

Thus, these events are a matter of concern for the governmental authorities together with their specialized security services. They can also be at the crossroads of the scientific and technical advances, inter alia in the field of dispersion and radiation modelling. Indeed, decision-makers need reliable, and preferably quick, health impact assessments of the events mentioned before to take proper protection measures of the people. Nowadays, such accurate assessments may be drawn on 3D modelling capabilities and computational resources that have been drastically improved in the last decades. The paper and presentation will develop three topics illustrating the input of modelling to nuclear / radiological security.

(1) Dispersion modelling in complex environments – Urban districts and industrial plants concentrate most of the economic activity and a large part of the population and are thus likely targets. They deserve a special attention, all the more that modelling the dispersion in such areas is very complex due to the influence of the topography and the intricate buildings geometry in evolving meteorological conditions. To address this critical issue, a toolbox of generic and flexible models has been developed by the CEA to evaluate the dispersion (and irradiation) of radionuclides from the regional scale to the local scale, and especially around and inside buildings, and critical infrastructures as the case may be. The models account for the effects of the buildings on the local flow, dispersion, deposition and irradiation, as well as the indoor/outdoor (or vice versa) transfer of radioactive materials. Computations are carried out in 3D with high space and time resolution in all the potentially affected area.

(2) Radioactive / nuclear source term estimate – In several cases, the irradiation or release by the source can be surreptitious without immediate obvious trace (like smoke or an explosion). However, the presence of the source may be detected by a network of sensors or people in trouble. Then, the quick and efficient identification of the source location and strength is of vital importance for the security teams. Once more, mathematical methods developed by the CEA can help in reconstructing the source term parameters, given a set of measurements coming from sensors. The probabilistic Bayesian approach combined with the retro-dispersion modelling yields several upsides as it allows the incorporation of model and observational uncertainties and the use of prior information if any about the source. While this approach was validated against measurements adapted to benchmarking source term estimate methods, it was also applied to realistic situations in complex built-up landscapes.

(3) Models “in-depth” validation – Even now it remains very challenging to model environments with complex characteristics, more specifically within and around buildings in urban or industrial areas.

Last years, European and international activities (like the European COST Action ES1006 or the UDINEE exercise) were dedicated to validate models against experiments with an increase in the complexity level, from idealized to realistic urban mock-ups, from wind tunnel scale to full scale real situations, from continuous releases to highly variable puff releases, and from simplified to full CFD models. The performances of the CEA models were evaluated through statistical analyses.
proving that they are compliant with the validation criteria, established in literature for complex environments. Moreover, in the interest of the benchmarking exercise, computations with the CEA modelling system were carried out by three independent teams of modellers making different parametric choices, therefore pointing out the robustness of the CEA models.

After commenting on the topics (1), (2) and (3), the paper and presentation give feedback and guidance about several concepts of use of models integrated in decision-support systems. For the purpose of planning and emergency preparedness, modelling is of help in the development of evacuation routes and procedures or the optimal design of detection networks inside and around critical infrastructures or urban districts. Furthermore, in the course or the post-event phase of a nuclear / radiological emergency, modelling can support rescue teams in improving their awareness of the situation and deciding if, when, and where counter-measures should be taken. To sum up, the CEA modelling toolbox has worthy properties of timeliness, accuracy, reliability, and relevance making the models qualified and a real benefit for nuclear / radiological emergency preparation and response. Moreover, the soundness of the approach developed in the last decade translates into increasing appreciation and trust of the emergency players for state-of-the-art 3D simulations to diagnose and anticipate critical situations.

State

France

Gender

Male

Primary authors: Dr ARMAND, Patrick (CEA); Mr DUCHENNE, Christophe (CEA); Mr PATRYL, Luc (CEA)

Presenter: Dr ARMAND, Patrick (CEA)

Track Classification: CC: Emergency preparedness and response and nuclear security interfaces
NUCLEAR SECURITY PROJECT FOR A BRAZILIAN FACILITY

Monday, 10 February 2020 12:15 (15 minutes)

This paper describes the application of a risk management performance-based approach, and compares a security project using three areas of nuclear security: physical protection, information security and accounting and control of nuclear material. This approach uses probabilistic threat parameters, equipment, systems and response forces used to prevent, dissuade and deter malicious acts against the integrity of nuclear facilities and its materials contained therein. Today, in Brazil, nuclear risk management uses a traditional prescriptive-based approach. This methodology does not take into account the current capabilities of the different internal or external threats to facilities. In addition, it does not provide system performance metrics in the face of such threats. Once the plans and systems that currently exist in real facilities must remain confidential, a hypothetical facility was developed, contemplating a small modular reactor. The use of the methodology made it possible to identify vulnerabilities of the model itself, given the needs of each of the areas of Nuclear Security. The results obtained shown us that the adoption of a performance-based methodology represents a significant evolution in the evaluation of physical protection systems, but it is not enough without being integrated with the areas of cyber-security and nuclear material accounting and control.

State
Brazil

Gender
Male

Primary authors: Dr BATISTA FIEL, João Claudio (Military Institute of Engineering); Ms R. DOS SANTOS, Pedro Maciel (Instituto Militar de Engenharia)

Presenter: Dr BATISTA FIEL, João Claudio (Military Institute of Engineering)

Session Classification: Physical protection systems: evaluation and assessment

Track Classification: PP: Physical protection systems: evaluation and assessment
Recent changes in National Legislative and Regulatory Framework for the Physical Protection of Nuclear Material in Use, Storage and Transport and for Nuclear Facilities: Finland

T. Hack, P. Karhu
Radiation and Nuclear Safety Authority (STUK)
Laippatie 4, P.O. Box 14, 00881 Helsinki, Finland

Abstract. Regulatory framework for the physical protection of nuclear material in use, storage and transport and for nuclear facilities in Finland consists of two main areas: combating crime and regulatory control of the use of nuclear energy and radiation. The primary responsibility for the security of a nuclear facility is appointed to the operator. In transport of nuclear and other radioactive material the cooperation is important, because the activity is not limited to restricted security zone. For all security activities, the national legislative and regulatory framework is a key aspect to ensure security against malicious and other illegal acts by insiders or outsiders, or both.

1. Introduction: link between nuclear security and national security strategies

Aspects of nuclear security are included in two national security strategies that are frequently maintained: [1-2]. The nuclear security regime in Finland is in line with these two strategies including the concept of cooperation between authorities. The requirements in the design basis threat (DBT) are based on national threat assessment for use of nuclear energy, including transport of nuclear material. This paper demonstrates how national legislative and regulatory framework in the field of nuclear security in Finland has been arranged and maintained.

1. The importance of security measures and the threat assessment

Preventive, detection and delay measures are important for nuclear security and for the comprehensive security arrangements. Basis for preventive measures is the national threat assessment developed by the Finnish Security Intelligence Service (SUPO) in cooperation with other relevant security authorities.

According to Nuclear Energy Decree [3], SUPO is responsible for threat assessment and STUK is responsible for developing a DBT. In Finland, the DBTs is developed of progressive levels of threat. Nuclear facilities have been divided into three categories based on the potential consequences.

Preventive measures are not only important against the outsiders, also the insider threat and collusion between insiders and outsiders must be considered. In the Finnish legislation there are several requirements and measures against both insiders and outsiders and both threats are also covered in the DBT. Required measures may differ based on the activity, e.g. operating a nuclear facility may require measures that are typically quite stable, but transport activities may require ad hoc type measures.

1. Development and maintenance of regulatory framework

Continuous development of a regulatory framework requires continuous assessment of threats both nationally and globally. STUK observes both national and global trends and revises the regulatory framework based on the changes in the threat environment. The current regulatory guides
and DBT for nuclear security were published December 2013, and the STUK regulation on nuclear security in 2016. Changes in the threat environment cause revisions of these requirements. The national legislative and regulatory framework for nuclear security in Finland is based on the pyramid model from the bottom (regulatory guides) to the top (constitution).

In the revision of the national legislative and regulatory framework, the CPPNM, as Amended, has been taken into account. During the gap-analysis of national legislative and regulatory framework, the needs for changes in the legislation have been identified.

During the 2019 revision of national legislative and regulatory framework, STUK has identified new threats and topics that must be covered in the regulatory framework. Use of drones, trustworthiness for sub contractors, up-to-date powers for security personnel and psychological evaluation of specific employees of the operator are examples of these. The objective is to maintain a comprehensive legislative and regulatory framework for nuclear security based on the current threat environment also in the future.

Legislative measures have been taken to ensure that the response of both operators and authorities against the malicious and other illegal acts is effective. However, organizational changes have an effect on how knowledge of special circumstances and operation in of a nuclear facility can be maintained in the police organization. Therefore, both joint exercises and working groups involving different authorities have been arranged. It is not unusual to have e.g. police special units, The Finnish Border Guard special units and The Defence Forces special units to exercise together with operator’s security organization. There must be a clear chain of command and an understanding of the roles of different parties in these circumstances to ensure decision making. Legislative measures are also in place to allow the parties to take necessary action. The significance of these exercises is important to recognize in the future, too.

References

State
Finland

Gender
Male

Primary authors:  Mr HACK, Tapani;  Mrs KARHU, Paula
Presenter:  Mr HACK, Tapani

Track Classification:  CC: National nuclear security regulations
Niger’s Experience in Establishing and formalizing nuclear security processes in integrated management systems

I. Introduction:
• An overview on Niger Republic and its related Nuclear Security activities.
• An overview of Niger’s legislative and regulatory framework of the field of Nuclear security
• the creation of a high level body coordination for Nuclear Security and the promotion of peaceful use of nuclear energy (HANEA)
• the creation of a National Comity of Nuclear Security within the HANEA.

II. Establishment of Nuclear Security activities through the National Comity of Nuclear Security:
• The adoption of a ridge of the Minister-in-Office of the President of the Republic determining the missions, the composition and the functioning of the National Nuclear Safety Committee;
• The allocation of resources for the functioning of the committee
• The official designation of focal points of national institutions with responsibilities for nuclear safety;
• The organization of the committee
• The development of an action plan to develop the national nuclear safety regime.
• The division of roles within the committee
• Drafting of activity reports in order to inform the highest national authorities about the activities carried out by the committee, the prospects and the challenges to be met.
• The integration of nuclear security into the implementation of national homeland security and the use of existing security systems for the benefit of nuclear security;
• Assessment of the national nuclear security system to identify strengths, weaknesses and challenges

III. The role of the IAEA in supporting the work of the committee:
• Training of committee members and other stakeholders in national, regional and international workshops;
• provision of reference documents to support activities;
• Expert missions;
• The Bilateral Cooperation Framework (INSSP), the other IAEA-Niger collaboration platforms, as well as the nuclear security networks (NSSC Network, FLO Network, etc.) allowing Niger to benefit from the experiences of other member countries of the IAEA.

IV. The successes registered and difficulties encountered:
IV-1. Successes related to the creation of the coordinating authority and the national nuclear safety committee
IV-2. Difficulties encountered by the committee in the implementation of its activities

V. Conclusion-Recommendations

State
Niger

Gender
Male
Primary author: Mr YAHAYA BAKO, Abdou Salam (Haute Autorité Nigérienne à l’Energie Atomique)

Presenter: Mr YAHAYA BAKO, Abdou Salam (Haute Autorité Nigérienne à l’Energie Atomique)

Track Classification: CC: Establishing and formalizing nuclear security processes into integrated management systems

The Integrated Nuclear Security Support Plan (INSSP) is a useful tool for Myanmar to develop and sustain national security regime with a comprehensive ways and systematic approach. Myanmar held finalization meeting for INSSP in November, 2013 and it was approved in July, 2015. After identification for gaps and needs of national responsibilities, prevention and reducing the risk, responding threat and obligations of international commitments for nuclear security through INSSP, Myanmar has been implementing to strengthen functional areas since 2013. Myanmar makes continual effort on strengthening legislative and regulatory framework through the international legal framework for safety, security and also safeguards activities. On the other hand, Myanmar emphasizes on effective prevention, detection, emergency response plan and capacity building program on nuclear and other radioactive materials with the close cooperation of national competent authorities with the assistance of IAEA and potential partners.

Myanmar has no research reactor or power reactor and their related facilities and activities but the use of radioactive sources which are mainly used in industry, medical practices and research academic are increased about three times within a decade. Myanmar government increases awareness on requirements of effective national nuclear security for nuclear and other radioactive materials in use, storage and/or transport and its associated facilities.


Atomic Energy Law was promulgated in June, 1998 and under the law, Division of Atomic Energy is doing regulator body’s functions as national registration, authorizations, inspections, enforcement, conducting capacity building training for relevant organizations and radiation users and establishing website for public information. Myanmar Counter Terrorism Law which is based on UNSCR 1373 and UNSCR 1540 for nuclear materials and facilities issues was enacted in June, 2014. The first priority area is to strengthen legal framework that new Nuclear Law is being drafted with the adequate provisions of nuclear safety, security and safeguards and it is now final stage to submit parliament.

In addition, Myanmar makes high priority areas for physical protection system for radioactive sources and its facilities, detection system for important border points and seaports, capacity building for emergency response team in close coordination with relevant entities and organizations. Myanmar has made awareness, outreach and engage program for national competent authorities for nuclear security activities in physical protection, DBT, orphan source search, detection and response with the assistance of IAEA and US-DOE, ANSTO and CBRN risk mitigation with EU-CoE. The advantages of INSSP implementation for Myanmar are increasing the role and responsibilities of coordination body, strengthening legislative and regulatory framework with adequate provisions, adopting legally binding and non-binding international instruments, designing and maintaining appropriate physical protection measures, developing national nuclear security detection architecture and developing human resources to sustain the security regime. Myanmar is now preparing to review and update the INSSP for further implementation to develop and sustain its
national nuclear security in 2019.

The paper presents developing and sustaining national nuclear security through the implementation of Integrated Nuclear Security Support Plan (INSSP) in close coordination with relevant national competent authorities and international organizations mainly IAEA and bilateral partners.

**State**

Myanmar

**Gender**

Female

**Primary author:** Ms OO, Lei Lei (Ministry of Education (Science and Technology))

**Presenter:** Ms OO, Lei Lei (Ministry of Education (Science and Technology))

**Track Classification:** CC: Identification of national needs through the development of an Integrated Nuclear Security Support Plan
Incidents of radioactive material out of regulatory control in Vietnam

Vietnam Agency for Radiation and Nuclear Safety (VARANS) is under the Ministry of Science and Technology (MOST) and has the responsibility to assist the Minister in performing the duties and authorities in radiation and nuclear safety; security of radioactive sources, nuclear materials, nuclear facilities; international safeguards; emergency response to radiation and nuclear incidents within its competency.

In database of radioactive sources in 2017, Vietnam has approximately 650 radioactive sources facilities with 5300 sealed radioactive sources, including about 2450 sources are in use and 2850 sources are in temporary storage. These sources are being applied in industrial, medical, research, education, and other purposes. Besides the benefits, radioactive sources also bring potential risks if not managed well. Currently, Vietnam does not have a national long-term storage of disused radioactive sources with sufficient capacity to manage a large number of radioactive sources, ensuring safety and security. The mainly disused radioactive sources are still stored in facilities and some units of the Vietnam Atomic Energy Institute are allowed supporting temporary storage. This has negatively affected the management of safety and security of radioactive sources, potentially high risk of loss, or theft of sources that can occur as incidents occur during the time recently.

From 2005 to now, there were 6 typical incidents of loss radioactive sources in Vietnam. The incidents of losing radioactive sources at facilities show that: The management system at facilities still has loopholes; The responsibility of facility for ensuring radiation safety and security of radioactive sources is still low; The process of managing radioactive sources is loose; Emergency response to incidents of loss radioactive sources is still slow and no close combination between the facilities and the regulatory agencies.

Reconsider the above-mentioned loss of radioactive sources, lessons learned after the incidents, as well as making corrective measures to enhance the work of ensuring radiation safety and radioactive source security, the Regulatory Agency in Vietnam has focused on the following issues: 1) Enhance inspection, verification to ensure the security of radioactive in Vietnam. When conducting inspections, there must be contents on security of radioactive sources, in which the existence of radioactive sources must be verified. Establish a national database of radioactive sources. Strengthen coordination between relevant ministries, branches, People’s Committees of provinces and cities in radioactive sources security. 2) Strengthening the capacity of VARANS and local Agency to well perform the function of managing radiation safety and security of radioactive sources, ensuring human resources, infrastructure and equipment for inspection activities and management, focusing on staff training. 3) Strengthening propaganda, dissemination and guidance on the implementation of legal regulations, training and awareness rising on radiation safety and security of radioactive sources for organizations and individuals in the local area. 4) Raising awareness among leaders and employees of the facility about responsibility for ensuring radiation safety and security of radioactive sources, building safety and security culture, focusing on training employees on radiation safety and security of radioactive sources. 5) Need to build a national storage facility to meet the requirements of safety and security management of disused radioactive sources.

State

Viet Nam
Gender

Male

Primary author: NGUYEN DINH, Giap
Presenter: NGUYEN DINH, Giap

Track Classification: CC: Information exchange for incidents of nuclear and other radioactive material out of regulatory control
HELINUC: Airborne gamma mapping system of CEA

HELINUC: Airborne gamma mapping system of CEA

Marine WANSEK, Stéphanie MENARD
CEA, DAM, DIF, Bruyères-le-Châtel, 91297 Arpajon Cedex, France

The CEA DAM has a number of high-capacity (2 – 20 liters) sodium iodide gamma detectors and high performance germanium detectors used for operational response in nuclear security events. The detectors are positioned in packaging adapted to their use: transport suitcases, measuring container... The knowledge of the energy response and the minimum detectable activities of these systems make it possible to ensure the adequacy of their employment to the needs.

One of the systems is the HELINUC Airborne gamma detection System. The container is loaded with 4*4 liters of sodium iodide scintillation detectors. Two germanium detectors installed on either side of the container can also be deployed. HELINUC is developed and implemented by the CEA/DAM at the benefit of the French nuclear intervention actors (Ministry of interior, Ministry of Defense), civilian nuclear operators (GIE INTRA), national public authorities and international agencies (IAEA...).

The missions of HELINUC are:
• The realization of radiological references of large agglomerations, civil and military installations
• Securing Major Events
• Emergency response in case of incident/accident at a civilian or military site and the search for emission points
• Searching for Point sources
• International assistance.

During a flight mission, gamma detected by the Helinuc system come from:
• Natural radiation sources (cosmic rays, natural terrestrial radionuclides ...)
• Industrial activities (phosphate processing, building materials, waste ...)
• Radionuclide release of nuclear accidents : 137Cs in soil ...

Two supplemental type certificates (STCs) validated by the European Aviation Safety Agency (EASA) in 2016 allow the installation of the HELINUC system on two types of helicopters: AS 355 and EC 145. CEA/DAM obtained a PART 145 agreement in 2018 to maintain the components of these two STCs.

Every day three persons from CEA are on duty (24h/7d) and ready to operate in case of emergency in France. The presentation will focus on
• The presentation of the HELINUC system
• The examples of airborne gamma mapping surveys
• The challenges of the training of the HELINUC team
• The challenges of an operational system

HELINUC has been operated in France since 36 years, and is continuously improved in the CEA laboratory. HELINUC is used in routine in France to perform between 3 and 5 surveys per year of French nuclear sites. There are two objectives for these surveys: first to evaluate the impact of the site on its environment, and secondly to establish a baseline which would be used as a reference in case of emergency.

State
France
Gender
Female

Primary authors: WANSEK, Marine; MENARD, Stephanie (CEA)
Presenter: WANSEK, Marine

Track Classification: CC: Emergency preparedness and response and nuclear security interfaces
Board of Radiation and Isotope Technology (BRIT) is engaged in production and supply of various radiation based equipment such as laboratory irradiators, blood irradiators, radiography devices etc. These devices are used in various institutions such as university, hospital and industries. Different sources such as Co-60, Ir-192 and Cs-137 etc. are used in these devices. These radiation based devices with source are transported in the public domain and they are kept in the universities, research center, hospitals etc. without much security. Hence, these radiation devices are much more vulnerable to sabotage than other devices which remain in nuclear establishments. Security of sources in these devices becomes more important. Graded approach has been followed in the design with the principle of deter, detect & delay to enhance the security of these sources. It is important to ensure securities of these sources not only during transportation but also at the installation site. Different design features are being incorporated in various new devices manufactured by BRIT to increase the adversary time.

Gamma Chamber which is widely used in universities and hospitals & research institutions was studied for its security hardening. These equipment are self-shielded devices in which a number of Co-60 source pencils are placed in a cylindrical cage. The Gamma Chambers are type approved as equipment and as a transportation package conforming to various national and international safety standards. But these Gamma Chambers were not earlier designed keeping in view the security aspects which has become more relevant now. There is need to secure such devices against different malicious acts. The acts may include theft of the radioactive material or attempt to break the shielding with the aim to spread the radioactive material. A mock drill was conducted to remove the sources from the Gamma Chamber at the installation site. Two people were given a basic idea of the equipment, a few tools and a drawing to take away the source and record the adversary time. Based on the mock drill a number of design features such as hidden fasteners, higher number of fine threaded screws, stopper plug, specialized tool for removing radiation source etc. are incorporated.

This paper covers details on the mock drill conducted on the Gamma Chamber and a number of modifications which have been carried out in the design of these equipment to increase the adversary time such that it is greater than the expected response time. The study will help in design modification of similar equipment carrying radioactive material.

Keywords: Gamma Chamber, Response time, Adversary time

State
India

Gender
Male

Primary author: Dr SAHOO, DHIREN (BRIT, DAE, INDIA)

Co-authors: Mr SRIVASTAVA, PIYUSH (BRIT, DAE, INDIA); Dr KOHLI, ANIL (Former CE, BRIT, DAE, INDIA); Mr GANESH, G (BRIT, DAE, INDIA)
Presenter: Dr SAHOO, DHIREN (BRIT, DAE, INDIA)

Track Classification: CC: Good practices in the development and execution of nuclear security exercises (e.g. tabletop, drills and field exercises);
Mitigation of Insider Threat by Enhancing Human Reliability Program

Jordan remains one of the new comer countries in nuclear projects, Jordan Research and Training Reactor is considered the first nuclear facility in Jordan. The security of nuclear facilities has been one of the challenges facing the Jordanian nuclear project as Jordan is a stable country located in a volatile area (Middle East.) Therefore, we have worked hard to maintain the security for the first nuclear facility in Jordan for all nuclear security aspects: Physical security, Cyber security, Security Culture and Human Reliability Program.

The human side in nuclear security is one of the most complexes in all nuclear security aspects; especially for insider the facilities (Employees, Contractors, Visitors ...) which called insider threats whether it is (intentional or unintentional)

The Paper will discuss the Jordan’s experience in mitigating the threat of insiders by strengthening the human reliability program through development of:
- Clearance and security check procedures
- Psychological & Medical Test
- Drugs Test
- Alcohol Test
- Awareness Programs

furthermore, the Paper will highlight the challenges during the implementation of the HRP.

State
Jordan

Gender
Male

Primary author: Mr ASSAF, Mahmoud
Presenter: Mr ASSAF, Mahmoud

Track Classification: PP: Insider threats
Change management - from the expectations of the competent authority to the implementation by the operator

Nuclear power plants and fuel cycle facilities are constantly changing, particularly in recent years with works related to the implementation of security reinforcements. The security of a facility can be weakened by a lack of anticipation of the potential impacts of the changes implemented on the facilities, in particular those relating to physical protection systems.

The French nuclear security competent authority has set a regulatory framework for enabling changes that could have an impact on security on site. The requirement set in the regulation concern modifications affecting one of the elements taken into account to license the operator. The regulation notably introduces the notions of simple information of the authority and authorization required before starting the works.

This general requirement takes into account the change in a large way and does not give any detail on the type of information to be transmitted according to the type of change, nor the nature of demonstration that this information should include.

In regards to nuclear security, the first major questions to consider before implementing works are:
- do the works improve security?
- do the works weaken security?
- in the latter case, what compensatory measures are planned?

The French nuclear security competent authority wants to constantly empower the license holder, that’s why a collaborative work has been set up with the operator Orano to define a guide dedicated to the management of changes for the different nuclear sites it operates. The aim of this guide is, for each facility, to know what information the operator has to communicate to the authority before beginning the works. This information should systematically include the answer to the previous three questions. In addition, for changes which are not relating to physical protection, the operator has to be able to explain to what extent security by design has been taken into account.

In order to have a pragmatic and proportionate approach, the guide defines different levels of changes and associated instructions, ranging from minor modifications than can be implemented without notice to the competent authority to substantial changes for which prior authorization must be obtained before the works start.

The presentation aims to share the approach used with Orano:
- the guide used to manage changes on site,
- the nature of information required according to the type of works planned,
- the collaborative work done with the competent authority, through technical meetings
- the benefits of this process.

It should be noted that the approach used with Orano which operates fuel cycle facilities is relevant because it can be used with any other operator and could particularly benefit other countries which need to manage changes on the facilities, including nuclear power plants and research reactors.

State
France

Gender
Female

Primary author: Mrs BARRAULT, Anne-Emmanuelle (Ministry for an Ecological and Solidary Transition)

Presenter: Mrs BARRAULT, Anne-Emmanuelle (Ministry for an Ecological and Solidary Transition)

Track Classification: CC: Implementation of national legislative and regulatory frameworks, and international instruments
Significance and Challenges of Physical Protection Systems Effectiveness Evaluation for Nuclear Material and Nuclear Facilities

Monday, 10 February 2020 12:30 (15 minutes)

Provision of nuclear materials and nuclear facilities physical protection is an essential part of nuclear activity. This statement mentioned in many IAEA International Documents. In particular, those documents also mentioned that modern physical protection systems (PPS) creation should be based on their effectiveness evaluation. It is necessary to understand how nuclear materials and nuclear facilities protection have been enhanced for some financial and human resources investment into PPS upgrading. This paper analyzes IAEA Nuclear Security Series (NSS) documents (NSS 13 "Nuclear security recommendations on physical protection of nuclear material and facilities (INFCIRC/225/Rev.5)", NSS 14 "Nuclear security recommendations on radioactive material and associated facilities", NSS 27 "Physical Protection of Nuclear Material and Nuclear Facilities (implementation of INFCIRC/225/Rev.5)") requirements concerning physical protection systems effectiveness evaluation. The paper views methods that were developed under Coordination Research Project (CRP) "Nuclear Security Assessment Methodology (NUSAM)" (2014-2016). Russian theoretical and practical experience in this area viewed as an example. It’s also mentioned evaluation methods were developed only in relation to physical protection systems but similar methods for following nuclear security subsystems (cyber-security etc.) are absent. Besides necessity of such methods development here viewed other perspective research trends. In particular here proposed to consider modern threats in detail (for example, unmanned airborne vehicles, divers, modern software/hardware used by intruder etc.) and their influence on nuclear facilities physical protection effectiveness. Furthermore the paper encourages other perspective research trends in this area: distribution of developed effectiveness evaluation methods to radioactive materials and associated facilities, human factors taking into account in physical protection systems effectiveness evaluation, optimization methods development for PPS design process (for example, by “cost-effectiveness” criteria), risk assessment methods development etc.

Key words: nuclear material, nuclear facility, physical protection, physical protection system, effectiveness evaluation

State

Russian Federation

Gender

Male

Primary author: IZMAYLOV, Alexander (JSC "FEDERAL CENTRE of SCIENCE and HIGH TECHNOLOGIES "SNPO "ELERON", Russian Federation)

Presenter: IZMAYLOV, Alexander (JSC "FEDERAL CENTRE of SCIENCE and HIGH TECHNOLOGIES "SNPO "ELERON", Russian Federation)
GIES "SNPO "ELERON", Russian Federation)

**Session Classification:** Physical protection systems: evaluation and assessment

**Track Classification:** PP: Physical protection systems: evaluation and assessment
Nuclear CyberSecurity considerations.

Cybercrime is widespread and rapidly increasing unabated in many institutions, government departments and in the private sector, as they are at odds in finding effective cybersecurity strategies to combat the new vice. The threats of nuclear attacks backed-up by cyber espionage have become a global issue to which the rate in is rising exponentially.

My concern is to address the challenge on nuclear cybersecurity, backed up by any form of attack. The vulnerability in IoT (Internet of Things) devices, scarce cybersecurity experts, lack of cybersecurity awareness and significant growth in Internet penetration are issues creating new opportunities for different types of attacks. I currently work at Radiation Protection Authority of Zimbabwe, a regulatory body that ensures the safe use of radiation and enforces nuclear security. A lot of sensitive data is captured, stored and consumed and it is our mandate to keep it safe and ensure the CAI (confidentiality, availability, integrity) triad within business processes.

Cybersecurity challenges are relatively new issues in Africa at large, which is unprepared and ill-equipped to handle threats of cybercrime. The risks posed by cyberattacks include exposure of nuclear sensitive information and sabotage of industrial control systems and physical protection systems. The INSSP (Integrated Nuclear Security Support Plan) recognizes the rise of digital intruders and now included the Nuclear Security Area 6 and it is imperative that even though we invest in State-of-the-art physical protection systems, decision makers should also address cybersecurity at their level and cascade it downwards for implementation. Systems are as strong as their weakest links (human beings if they lack training, but can be great assets if properly trained). Workers at nuclear facilities should develop an optimum cybersecurity culture and only then will we be able to combat digital intruders. The development of the IoT, which enables communication between machines, raises the possibility of appliances being manipulated by hackers remotely. The widespread use of machine-to-machine communication is only likely to boost information misuse and users of these systems should be aware of such vulnerabilities and try and conform to the international best practices of cybersecurity.

Most facilities that handle radioactive materials have inadequate UTMs (unified threat management) systems. Cyber security requirements for a network should include at least Endpoint Protection, UTMs, Radius Server, Logging Software or Encryption. In addition to that, devices should be configured with experts, and training administered to personnel in charge of systems security.

Awareness training for all employees is necessary as a foundation and entry point for cybersecurity adoption. Traditional IT security practices like network monitoring and segmentation have become even more critical as businesses and governments deploy IoT devices. Cyber insurance plans should be put in place to cover a variety of costs related to cyber-attacks.

It is very much possible to employ machine intelligence mechanisms to enhance nuclear cybersecurity at facilities. Facilities that use nuclear material have certain information that they have, depending on their sources’ categories and their computer interaction patterns, Big Data can be used to make this unstructured data computer readable and enable the effective use of this data by the regulator and the state. Machine learning concepts and Big Data can be used to counter our problems within SOCs (security operations centres) as well as enhance nuclear security detection architectures. Machine learning algorithms can be used to support Big Data by learning the vulnerabilities and ransomware trends, and coming up with ways to guard against digital intruders. There are over 1000 facilities in Zimbabwe that use radioactive material, and a security breach of any of these facilities could cause a catastrophic nuclear security accident. The risk of such an event is always there and the challenge is that, RPAZ has no idea as to which facility is engaging
in practices that can compromise nuclear security. Big Data is the can then be used to analyze
digital trends within organizations and use machine learning algorithms to come up with ways
to determine facilities that are bound to compromise nuclear security and proactive measures are
taken immediately as opposed to reactive measures, thus, ensuring nuclear security in Zimbabwe
and the world at large.
Nuclear Cybersecurity is one of the most urgent issues worldwide. Computer networks have al-
ways been the target of criminals, and the danger of nuclear security breaches will only increase
in the future as these networks expand, but there are sensible precautions that organizations and
states can take to minimize losses from those who seek to do harm. With the right level of prepa-
ration and specialist assistance, it is possible to control damages, and recover from a cyber breach
and its consequences. Cyber Security awareness is important in order for companies and individ-
uals to keep on guard against attacks. It may not happen imminently, but eventually a breach is
bound to suffice and one has to deal with the fallout.

State
Zimbabwe

Gender
Male

Primary author: Mr NDALAMA, Leenold Tinashe (Radiation Protection Authority of Zimbabwe)

Presenter: Mr NDALAMA, Leenold Tinashe (Radiation Protection Authority of Zimbabwe)

Track Classification: CC: Information and computer security considerations for nuclear security
French advanced reachback capability in support to R/N security

In France, the fight against illicit trafficking of radioactive and nuclear materials as long as the suitable operational response is part of the national security organization and doctrine. More widely, an efficient response to R/N terrorist threats requires coordinated actions from various authorities, such as security and control forces (mainly police and customs) or specialized units (fire brigades, ...), supported by R/N experts.

In the framework of this national organization, the military division of CEA (Commissariat à l’énergie atomique et aux énergies alternatives) is in charge of aspects related to R/N threat in different contexts, ranging from radiological and nuclear security of major public events and critical infrastructures to radiological and nuclear monitoring of national points of entry. For decades, CEA has provided expertise for the definition of suitable technical equipment depending on the operational context, operated fixed R/N detectors, deployed specialized operational teams, provided support and expertise to field teams and conducted research in R/N detection.

Due to that long-term experience, CEA was entrusted by the National Security and Defense Secretariat (Secrétariat Général de la Défense et de la Sécurité Nationale - SGDSN) to create a national reachback center at CEA to support authorities as technical experts in the management of R/N events. The first objective while facing a R/N event is to discriminate between situations related to health issues or malevolent threats, and thus scale the operational response depending on the type and level of threat.

The presentation will focus on operational missions of the national reachback center in:

- assistance to first responders (fire brigades, ...), in terms of radiation protection and analysis of data from spectrometric detectors, via the French TRIAGE, a remote analysis response specially designed to help any first responders facing R/N problems,
- contribution to the Inter-ministerial Central Detachment for Technical Intervention (DCI_IT), a structure dedicated to support the authorities in charge of a crisis. Depending on the categorization of the threat, specialized operational teams from DCI_IT (including teams from CEA/DAM) might be deployed to guarantee a suitable response to the event,
- monitoring of critical infrastructures or entry points (major public events, maritime ports, ...).

In particular, several relevant events and exercises will be presented, including the dual JRC/CEA demonstration performed at the "Magic Maggiore" GICNT workshop (Ispra, 2017).

These examples will illustrate the benefits of such centralization of expertise (minimization of infrastructure and maintenance costs, minimization of specialized manpower needs and associated training, ...) and minimal guidelines (adequation between deployed technologies and reachback level, 24h/24 network supervision to guarantee operational response, ...).
Male

**Primary authors:** MASSE, Daniel (CEA); PETITGUILLAUME, ALICE (CEA); SCHOECH, Hubert (CEA)

**Presenter:** MASSE, Daniel (CEA)

**Track Classification:** MORC: Detection technology development and performance testing
Simulations and tools in support to reachback experts

Providing an efficient response to R/N threats is complex and highly benefits from the existence of a fully integrated nuclear and radiological detection architecture. For decades, the military division of CEA (Commissariat à l’énergie atomique et aux énergies alternatives) has been involved in operational response to R/N terrorist threats. In 2014, the French authorities entrusted CEA to develop, maintain and run the National Center for Radiological Expertise (CNER – Centre National d’Expertise Radiologique).

During a R/N event, CNER experts will provide assistance to first responders and national authorities in terms of radiation protection and perform analysis of data from spectrometric detectors, either portals or handheld detectors.

The presentation will focus on some key support actions, which are primordial to maintain a reachback center, such as CNER, in an operational state:

- First, to guarantee the quality of received data, which conditions the relevance of the following expertise, key actions are:
  - upstream characterization of detectors on a metrology platform to refine technical awareness of detectors capabilities and limitations in operational contexts and to set suitable thresholds,
  - training of first responders on data acquisition conditions.

Indeed, thresholds optimization is very important to ensure effective monitoring of the site and minimization of innocent alarms rate. Therefore, innocent alarms or radiological detection that are qualified as “normal” (natural occurring radioactive materials below an acceptable level, radiopharmaceutical at a level compatible with in vivo administration …) do not lead to the interception of the monitored entity.

- Then, to expertise cases of complex radiological events that require high level training and experience, keys actions, such as are development and use of reference spectrum databases, analysis tools and simulation tools, highly benefit to CNER experts. Indeed, some R/N configurations can be reproduced on a metrology platform to acquire reference spectrum and characterize detectors performances. However, specific scenarios are impossible to reproduce with experimentations. Therefore, the creation and validation of models of detectors is essential to further characterize detectors responses and enrich a reference spectrum database.

To illustrate the importance of these simulations and tools in support to reachback experts, the methodology used to create and validate models of large volume detectors will be presented through the example of one specific detector. Then, a set of R/N event expertises, based on real data from the system deployed in Le Havre harbor, will be detailed to highlight the contribution of those models to the expertise of reachback center experts.

State
France

Gender
Female

**Primary authors:** PETITGUILLAUME, ALICE (CEA); Mr VAYRE, Sylvain (CEA); Mr MASSE, Daniel (CEA)

**Presenter:** PETITGUILLAUME, ALICE (CEA)

**Track Classification:** MORC: Detection technology development and performance testing
Computer-based systems have gradually replaced many of the mechanical and pneumatic control systems in research reactors and nuclear power plants. These systems have hardware and software components. Software updates are necessary due to the fact that at the point of software commissioning they may contain a number of undetected faults and cybersecurity bugs. These faults and bugs can lead to critical failures and cybersecurity vulnerabilities. Consequently, software update is crucial to resolve and mitigate these issues. Research reactors digital systems are subjected to changes, modification, and upgrading due to their extended usage and multi activities. But, gained experience from software updating highlighted the fact that sometimes software updating processes jeopardize the safety and vulnerable the cybersecurity of nuclear facility to cybersecurity attacks. There are some issues that should be addressed in more details when updating these digital systems. One important issue is the software updating planning where there are many factors that should be analyzed before starting the updating process. Another issue is the security of the updating process lifecycle to avoid the existence of new vulnerabilities which could be discovered and re-exploited by attackers. So, cybersecurity measures is an requirement to ensure that software update will improve system functionality which may be safety function or cybersecurity function or fix cybersecurity bugs which could be exploited by attackers. This paper discusses and analyzes the effect of software updating on safety and cybersecurity of research reactors from different point of views. Also, this paper proposes requirements and guidelines to avoid such drawbacks on safety and cybersecurity.

Software updates are necessary due to the fact that at the point of software commissioning they may contain a number of undetected faults, which can lead to critical failures of the fault tolerate critical systems. Assuring Safety and security are primarily based on keeping software updated for the critical system and are the first safeguard against cybersecurity incidents and events. Generally, a software update is a software file that contains fixes for problems. The updated process could be proposed by the software’s users or developers based on detected bugs, or cybersecurity risks. In nuclear field updated process could be required by regulatory body in response to learned lessons from events and accidents happened in similar systems of nuclear plants. Also, it could be new capabilities added to the original software. Installing an update fixes the code and prevents the bugs from affecting the plant computers. Software update is needed for many reasons, such as:

- Updates protect against new-detected security risks.
- They introduce new features in safety critical software.
- Software updates can improve combability between system equipment and between updated system and other systems.
- They extend the useable life of your equipment by allowing the maximum productivity from your equipment.
- Updates fix bugs in the software and improve functionality.

Although, there is an air-gap between the public internet and nuclear plant digital systems, these systems are still subjected to cyber-attacks. Air-gap is very easy to be breached with nothing more than a flash drive. It noted that the destructive Stuxnet computer virus infected Iran’s nuclear facilities via this route. Also, human factor cannot be neglected in such cybersecurity incidents. Both human and flash derive represent the bridge for malwares and viruses to cross the air-gap and attack digital systems in research reactors and nuclear power plants. This could be happened during software update and maintenance whatever unintentionally or intentionally by disgruntled employees, cyber criminals, state-sponsored hackers and terrorists. Two incidents related to software updated will discussed, one is concerned with safety and the other is concerned with cybersecurity attacks.

This paper proposes a framework for the software updating planning process of digital critical system (see Fig. 1) to avoid re-appearing cyber security vulnerabilities and errors and faults.
As cybersecurity regulations is still new topic to many regulatory bodies, this paper proposes a set of requirements to regulate the software updating process for safety and safety related digital systems:

1- Cybersecurity measures shall be in place through the lifecycle of software updating process.
2- Software updating shall be formally documented and approved in consistent with the software configuration management plan.
3- Software updating for safety and safety related systems shall be approved by regulatory body.
4- The software updating on safety and cybersecurity shall be implemented on simulator before its implementation on real systems.
5- The documentation shall include the reason for the change, identification of the affected software, and the impact of the change on the system including the hazards and risks analysis.
6- Additionally, the documentation shall include an updating plan for implementing the change in the system along with updating documentation including the hazards and risk analyses and additional software life cycle activities such as V&V.

State

Egypt

Gender

Male

Primary author:  SALLAM, Hany (Computer Engineering)

Presenter:  SALLAM, Hany (Computer Engineering)

Track Classification:  CC: Information and computer security considerations for nuclear security
Specifics of physical protection of CNST

1. General requirements to PP system and the site perimeter protection
Centers for Nuclear Science and Technologies (CNST), designed and constructed by Rosatom for foreign customers, usually contain: multipurpose irradiation center (MIC) with gamma-irradiator Co-60, pool-type nuclear research reactor (NRR) and proton cyclotron complex with medical laboratories. These installations are located at the CNST site in separate buildings. In accordance with the IAEA recommendations and guidance of Nuclear Security Series [1-4] the physical protection (PP) measures of CNST should take into account characteristics of nuclear and other radioactive materials and the associated facilities at the site. Following IAEA recommendations [3] on PP of nuclear material (NM), used for operation of the NRR at the site, the reactor facility should be protected within a limited access area (LAA). Gamma-irradiator facility, containing radioactive source (RS) of category 1, should be also in LAA, surrounded by a fence barrier with lightings and cable lines and equipped with access management tools at personnel and vehicle checkpoints.
Functioning of PP detection and delay equipment and guard/ response operations, require appointment and training of special facility protection forces, appointed by the State authorities. Number and required skills and competencies of these forces depend on PP system equipment and design basis threat, developed by the State Competent Authority.

2. Measures for protection of MIC
Gamma-irradiator of Co-60 of category 1 [1], e.i. the most dangerous type of RS. Access management measures for the irradiator include intrusion detection sensors and alarm assessment techniques along the MIC building perimeter and/ or fence, continuous observation of the radiation room and control of the source in operation and in its storage pool. Important is to apply CCTV monitoring of irradiation process when the source in use and access control with person identification biometrics.

3. PP sub-system of research reactor
Pool-type NRR of CNST is usually designed for thermal power of 0.1 to 10 MW and powered by low-enriched (near 19%) uranium fuel, containing category III [3] nuclear material of mass less 5 kg of U-235. It defines recommended measures against unauthorized removal (theft) of the NM. Measures against radiological sabotage of the NRR depend on its potential radiological consequences. Using IAEA example of graded approach [4], the reactor facility may be considered as sabotage category B facility, which does not require additional intrusion detection and access control measures in comparison with the theft prevention measures. As of response measures, the NRR protectors should be aware of adversary task time for sabotage, which is shorter than in case of theft.
Activity of radioisotopes, produced at the NRR facility, is usually below category 3 of dangerous RS [2] and require such a protection measures as inventory of irradiated targets (samples) and control of their transportation at the site and outside by radiation monitoring system.
PP measures for NRR building include access control, interior intrusion detection and alarm assessment cameras and procedures for transferring custody of the category III NM to the succeeding handler for protection from insider threat. Technical means and procedures for access control, such as keys and computerized access lists, protected against compromise and interior CCTV monitoring are also required.

4. Protection of cyclotron and the associated laboratories
The cyclotron facility and the associated laboratories do not operate nuclear material, nor very dangerous radioactive sources and will produce low-activity radionuclides for medical applications, e.g. diagnostics. Computerized inventory of produced radioactive materials (RM) and radiation monitoring at the facility site and in case of transportation outside CNST.
is strongly recommended. In addition, access control at the cyclotron entrance, locks at
doors and gates of the building are necessary for the cyclotron facility building(s).

5. Conclusion

Current PP system requirements are based of so-called “prescriptive approach”, described in
IAEA NSS #27 for NM category III facilities [4]. This approach is also suitable for protection
of irradiators and other radioactive sources of high activity [2].

Advantage of the “prescriptive approach is a relatively simplicity in understanding and ap-
lication of PP measures by nuclear operator and PP inspection by nuclear regulator This
approach is very useful for “nuclear newcomer” States, planning and constructing their first
nuclear research facility, but not experienced in “performance based approach”, requiring
development of DBT, for the site with access rights for multiple sub-contractors, service
providers, external medical personnel and patients. Finally, the prescriptive approach for
protection of CNST seems well justified.

References
3. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear
Facilities NSS #13, 2012.
4. Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision
5), NSS # 27, 2018.

State

Russian Federation

Gender

Male

Primary author:  Dr KRYUCHENKOV, Vladimir (Advisor, State Corporation Rosatom Rusatom Overseas)

Presenter:  Dr KRYUCHENKOV, Vladimir (Advisor, State Corporation Rosatom Rusatom Overseas)

Track Classification:  PP: Security by design, including in newcomer countries
ELEMENTS OF INTEGRATING SAFETY AND SECURITY DURING INSPECTION in Albania

Albania has established much of the legal and regulatory framework necessary to form the basis of a comprehensive security regime for radioactive sources and associated materials and facilities. The law establishes and empowers a regulatory authority Radiation Protection Commission to enact security requirements on licensees. The regulation on Physical protection of radioactive material require for licensing, inspection and enforcement for security of radioactive sources. The strategic objective of the Radiation Protection Commission, as the national independent authority, nominated by Council of Ministers, is the protection of health of the workers, public and environment ensuring safety and security, taking maximum benefits of using radiations. Albania is working toward implementations of the security series of IAEA. Key structure in the field of security are Radiation Protection Commission (RPC) and Radiation Protection Office (RPO), respectively as decision making and executive for the protection, as well as State Police, Custom etc. Adopted legislation in this area has been aimed to approximate IAEA and EU safety and security standards.

Executive Competent Authority is Radiation Protection Office responsible for inspection process for all category of radioactive materials all orphan sources. Inspection objective is that license keep authorization condition S&S Single and small regulatory programs implemented is better to have one inspection program form safety and security. The regulatory regime adopted depend on the size, complexity, safety and security implications of the regulated radiation practices and sources, as well as on the regulatory experience. The principal component of monitoring is on-site inspection, direct personal contact between operators and regulatory body’s personnel

Integrated because...
- Cost...
- Competence management of inspectors...
- Role of radiation protection officer and radiation security officer. (mainly form us is the same person with different duties.)
- Implication of safety from security and vice versa
- Implementation of graded approach on safety and security
- Implementation of safety principle and security recommendations

In the case of security, Albanian State police also determines the threat in a risk-based approach, and the associated nuclear security regime that needs to be implemented to deal with such a threat and its potential consequences. The prime responsibilities for implementing measures addressing safety and security measures to counter the threat rest licensee. Effective leadership and management to carry out these responsibilities needs to be established and maintained at all facilities and activities that involve radioactive material or give rise to radiation risks. Measures for controlling radiation risks (safety or security events) have to ensure that no individual bears an unacceptable risk of exposure and people and the environment, both present and future, are protected against unnecessary radiation risks;

Safety and security assessments and their associated radiation protection measures have to be conducted to a degree that is commensurate with the level of risk posed by the facility, by applying the graded approach. All practical efforts have to be made to prevent and mitigate radiological, security or radiation incidents/accidents by applying the principle of defence-in-depth, providing several layers and methods of radiation and physical protection. Emergency plans (called contingency plans for security events) for emergency preparedness and response for security or radiation incidents/accidents have to be in place

Main elements of security are ; Prevention detection, delay, response, and security management to be checked.
Inspections generally comprise:
(a) initial or pre-operational inspections carried out prior to a practice commencing work with radiation, sometimes required as part of the process of authorization including safety and security
(b) planned inspections of existing authorizations usually at specified frequencies;
(c) inspections with the purpose of making investigations when the RPO so deems necessary;
(d) inspections carried out following cessation of the radiation practice or if an authorization is otherwise cancelled

The regulatory body establish a planned and systematic inspection programme. The management of inspection activities is an important function, perhaps the most outstanding duty for the regulatory body from a radiation safety and security point of view.

Responsibility of inspector
• assuring his/her own adequate knowledge and appropriate training on inspection ;
• programming of inspection activities by establishing the appropriate priorities;
• developing guidelines for inspectors;
• determining whether an inspection should be announced or unannounced;
• assessing the resource requirements for the inspection programme (e.g. purchase and calibration checking of radiation detectors, expenses associated with inspectors’ travel, accommodation and incidentals, etc.) and assigning resources to the programmes in the annual budget;
• coordinating inspections with those responsible for assessing authorization applications and renewals;
• maintaining records of inspections (i.e. by correlative inspection number, and including full name of the facility inspected, date, starting and exit time of inspection, surname and name of inspectors);

Training
Inspection personnel must be capable of performing the tasks required by the inspection programme. The level and depth of training will also vary according to the duties performed and the potential hazards associated with the regulated radiation practices and sources in the respective country. Inspectors are to be provided with training that ensures they have understanding of:
• safety principles and concepts on safety and security (i.e. including hazards other than from ionizing radiation that may be encountered during inspections);
• monitoring instrumentation, detection techniques and procedures and operating techniques, etc

State
Albania

Gender
Male

Primary author: Dr PACI, RUSTEM
Co-author: Ms MURAJ, IDA
Presenters: Dr PACI, RUSTEM; Ms MURAJ, IDA
Track Classification: CC: National nuclear security regulations
Developing Security Processes for Critical Software System

Recently, many Nuclear Power Plants (NPPs) have been upgraded from analogue systems to computer-based control systems. The control systems perform data acquisition, control actuation, and information indication based on software. The digitalization of nuclear facilities has brought many benefits, including high performance and convenient maintainability, in terms of facility operation. With the growing trend in using safety-critical software as an embedded system in many critical applications in nuclear facilities, where such systems contain sensitive data and perform both safety and security functions.

Cyber security regulations require developing secure software development methodology for Instrumentation and Control (I&C) systems to prevent the digital system from cyber-attacks. I&C systems are considered to be the brain of the NPPs, and recently with the growing trend of using digital I&C systems, digital I&C systems are computer-based systems.

However, use of the digital I&C system can introduce the cyber security problem that may compromise important functions such as reactor shutdown or the mitigation of release of radioactive materials. Therefore, protection from cyber-attacks has been one of the key issues in nuclear facilities.

The unauthorized modification of these systems (in software or hardware) or disruption of its functions can significantly affect the plant operation. It may affect the plant safety in case of safety functions are affected or normal operation in case of safety-related or other control functions are affected. Consequently, Security became an essential requirement for developing critical software for such systems. So developing secure software is a critical issue, especially for NPPs. The impact of a software malfunction or security breach can result in loss of sensitive data, and system malfunctioning due to either intentional or unintentional interference. The consequence of such interference could be an accident or system fail to perform its intended protective action. Traditionally, security is usually unnoticed during the early phases of the software life cycle.

Unfortunately, Security testing performed near the end of the software development lifecycle, prior to deployment, but that process can put release schedules at risk and late-found defects cost more to address. However, there is still no clear software development process regarding security activities. Cyber security regulations require developing secure software development methodology for Instrumentation and Control (I&C) systems to prevent the digital system from cyber-attacks.

To more effectively address security, critical software system must be developed in a secured environment and each phase of software development should be designed, implemented, and executed under suitable security measures. In this paper, the main objective is to focus on security processes at each phase of the software development life cycle. An adapted V-model has been designed for developing secure critical software system where security deliverables are inserted in all phases of development. In adapted V model, security life cycle processes should be integrated into software development life cycle phases such as security requirements elicitation, definition, and analysis, secure design based on design principles for security, hazard analysis by using analysis tools, secure reviews and inspections, and security testing. This paper outlines the security attributes, activities, and procedures that should be inserted into all phases of software development life cycle for developing secure software that can stand up under attack, and provide confidence in the security-related properties and functions of the developed software.

State

Egypt
Gender
Male

Primary author: Dr SHAFEI, Ehab (Lecturer)
Presenter: Dr SHAFEI, Ehab (Lecturer)

Track Classification: CC: Information and computer security considerations for nuclear security
Testing facility for the qualification of measurement devices suitable for detecting nuclear and radioactive material

Fraunhofer INT has a profound long-lasting experience in the assessment of measurement devices for the detection of nuclear and radioactive material. This includes searching and identifying radioactive and nuclear material with hand-held and portable gamma and neutron measuring devices including electrically cooled germanium detectors. For example, the latter were investigated concerning the outcome of the implemented analysis routines and the obtained spectra which were examined using different further analysis tools.

Due to this long-lasting experience some researchers of the working group have been invited to participate as experts in the Illicit Trafficking Radiation Assessment Program (ITRAP+10). ITRAP+10 was a program initiated by the European Union and the United States to evaluate the performance of available commercial radiation detection equipment against consensus standards.

The ITRAP+10 effort accentuated the need to have accredited testing laboratories in the EU to perform testing against the consensus standards in order to have reproducible test results, independent of testing location. Therefore the next step is to enable laboratories to work as such testing locations. Initiated by the EU, this was carried out in ITRAP+10 Phase II in work package 2. Fraunhofer INT has conceived and built a test environment to perform the corresponding dynamic and static test measurements using neutron and gamma sources. This testing facility can be used to qualify new devices as well as to test already deployed ones. Therefore a reliable comparison between different devices is possible. This could be helpful for the procurement of additional components when the presently used version is no longer available or a replacement with new equipment has to be done.

The system for static measurements consists of a central cube for placing the radioactive sources. While not needed for the measurement, the source is moved down and shielded with a combination of lead and polyethylene, both borated and normal. Polyethylene is inserted for neutron sources used. A maximum shielding with a thickness of 15 cm and a height of 30 cm can generally be placed around the source using 5 cm x 10 cm x 20 cm bricks. If other thicknesses are needed, individual solutions can be realized.

Guide rails can be attached to the central cube, each of which has a roller carriage placed on it and can hold a measurement device. Their height can be adjusted which enables us to bring the center of the detectors to the same height as the center of the source. The roller carriages are fully adjustable via setting wheels. The roller carriages and the guide rails are equipped with scales for measuring distances. We have four guide rails which can each be placed on the sides of the cube or can be placed in a row in order to enlarge the distance from the source. The length of each guide rail is 1.5 m.

In order to measure the time behavior e.g. time to alarm or time to stabilize a measurement value, it is necessary to have a short lift up time for the radioactive sources. Intended times are below 0.5 s. Therefore a lift-up mechanism based on compressed air was chosen for the lifting device. The resulting lift uptime is about 0.35 s.

The tests performed at the static measurement system may include tests of general requirements, radiological tests, and radionuclide identification tests. The tests of general requirements in general involve tests of the user interface, battery requirements, and documentation of audible and vibrational alarms. The radiological tests comprise, for example, tests concerning false identification rate, time to alarm, accuracy tests for photons, and over-range and gamma response of a
neutron detector. The quality of the nuclide identification results is part of the radionuclide tests. The system for dynamic measurements consists of a roller carriage running on guide rails. The radioactive or nuclear material required for performance tests are positioned on the roller carriage at a variable height. This system is especially suitable for the qualification of portal monitors. The material in question passes by the monitor at a well-defined distance and height. Due to limitations of lab space, portal monitors for pedestrians are best suited to be qualified by the system. Possible aspects of qualification measurements include the behavior of the monitor’s occupancy systems, false alarm tests, response to gamma and neutron radiation, neutron indication in the presence of photons, over-range tests, and the determination of the vertical profile of the monitor. Both systems of the testing facility and their options for qualification measurements will be presented.

State

Germany

Gender

**Primary authors:** BORNHÖFT, Charlotte (Fraunhofer-INT); FRIEDRICH, Hermann (Fraunhofer-INT); Dr RISSE, Monika (Fraunhofer-INT); SCHUMANN, Olaf (Fraunhofer INT); KOEBLE, Theo (Fraunhofer-INT); BERKY, Wolfram (Fraunhofer INT)

**Presenter:** KOEBLE, Theo (Fraunhofer-INT)

**Track Classification:** MORC: Detection technology development and performance testing
Mapping National Legal Frameworks for Radiological Security

The hundreds of thousands of radioactive sources in use worldwide (in perhaps every UN Member State) pose a significant risk for misuse if not well-secured. Evidence from recent decades shows that some terrorists seek to cause mass casualties and mass disruption, and they have shown an interest in acquiring nuclear and radiological devices to such ends. Use of a radiological weapon by terrorists or other criminals would have an immense impact. A 2018 study by Sandia National Laboratories estimated the detonation of a Radiological Dispersal Device (RDD) using an IAEA Category 3 source in New York city would have a $24 billion impact and, although it would prompt no immediate fatalities, the evacuation would cause about 800 deaths (based on evidence from the Fukushima evacuation) [1]. As important, such an event would likely prompt international action – and likely over-reaction – to constrain trade in radioactive sources, a trade in which virtually every country participates and on which many lives depend.

In a paper presented at the 2018 International Conference on the Security of Radioactive Material, the Stimson Center identified a total of 248 national laws, regulations or their equivalents in 104 UN Member States that contained an obligation to secure or physically protect radioactive sources, apparatus or facilities [2]. Assessing those measures against 11 key elements in the IAEA Code of Conduct on the Safety and Security of Radioactive Sources, the paper revealed significant gaps existed in most national legal frameworks. In 2019, again with funding from the Government of Finland, the Stimson Center updated that database and built an additional database assessing related trade measures against the Guidance on the Import and Export of Radioactive Sources.

To provide new insights into implementation of the Code and Guidance, in this analysis the author prepared three composite indices of the national legal framework for securing radioactive sources, apparatus and facilities. The first composite index creates a score for each UN Member State based on the domestic-focused laws, regulations and similar measures in place, as updated in 2019, compared against 11 key elements of the Code. The second composite index creates a score for each UN Member State based on the national trade-focused laws, regulations and similar measures for radiological security compared against 15 key elements of the Guidance. The final composite index links those two scores for an overall radiological security legal framework score for each UN Member State. The author then uses choropleth maps (i.e., maps showing geographic areas, in this instance States, using a color gradient for a variable) to provide new insights into the index data, from geographic clusters to unexpected outliers. As much about implementation of the Code and the Guidance remain uncertain, the author sees this work as exploratory. The author hopes the analysis will help generate new hypotheses that will help the international community in its efforts to increase radiological (and nuclear) security.


State

United States
Gender
Male

Primary author: Dr CUPITT, Richard (Stimson Center)
Presenter: Dr CUPITT, Richard (Stimson Center)

Track Classification: CC: Implementation of national legislative and regulatory frameworks, and international instruments
A Maturity Model Method for Nuclear Security Program Assessment & Planning

The consequences of nuclear terrorism represent a grave threat to international security. The responsibility to address the risk of nuclear material theft or sabotage of nuclear facilities is shared by multiple organizations that must strategically collaborate based on their individual missions and capabilities. Stakeholder organizations share a common need to prioritize their activities based on threats, available resources, and existing security program maturity/capabilities, develop engagement plans and measure their progress - identifying milestones, measuring program performance, and communicating program impact is challenging.

However, the nature of improving security touches disparate, complex disciplines. The purpose of this paper is to propose and evaluate a methodology that will assist selecting long-term risk reduction goals and planning improvement activities across multiple security disciplines and stakeholder organizations. The methodology proposes maturity metrics to assess and communicate performance. The methodology is extensible to any security discipline and a cyber security example will be developed for demonstration.

Security Disciplines - A nuclear security program is composed of multiple security disciplines. These disciplines include Physical Protection, Material Control & Accounting, Cybersecurity, etc. To improve the security program, it is necessary to evaluate the disciplines individually and prioritize those areas that should have additional resources applied.

Discipline Domains - A domain is a logical grouping of common nuclear security practices that represent a core capability. For example, a core capability for a cyber security program is ASSET MANAGEMENT. A high performing cyber security program knows what hardware and software has been installed and manages those assets. Our process measures, tracks, and communicates improvement in maturity of identified domains.

Maturity Indicators - Maturity indicators are the observables that demonstrate security capability for a given domain. For each domain, there are multiple performance indicators to enable an assessment of capabilities. For example, does the site track assets? This would be one of many maturity indicators of an asset management program.

Maturity Levels - To simplify communication of goals, maturity indicators can be grouped into levels. Maturity Indicator Levels (MILs) describe a progressive step in a country’s capability and/or represent a demonstrated capability that is measured by the model. The proposed model would assign attributes, characteristics, and indicators that represent fundamental capabilities within a domain – Maturity Indicator Levels (MILs).

Stakeholder Engagement Activities - For each domain and maturity level, multi-stakeholder actions are identified based on standards, best practices, or country-specific goals. The stakeholder engagement activities matrix has two important features:

• It can be adapted to different levels: international organizations, nation state, regulatory agencies, individual organizations, etc. It is not specific to just one organization. Rather it proposes specific actions for all potential stakeholders such as government and regulatory agencies, industry working groups and international organizations. This is an important feature as it represents the breadth of potential resources and shows how organizations need to collaborate.

• It is based on the necessary maturity level specific to the security discipline and domain. This delivers action plans that are at the right level and can evolve over time as security maturity develops.

This method is actively being developed and piloted in the US Department of Energy International
Nuclear Security program so our paper will include an evaluation and lessons learned from the pilot - what works, what doesn’t, challenges in implementation, etc.

State

United States

Gender

Male

Primary authors:  DAWSON, Lon (Sandia National Laboratories);  WHITE, Greg (Lawrence Livermore National Laboratory);  NICKERSON, Charles (Idaho National Laboratory);  CLEMENTS, Samuel (Pacific Northwest National Lab)

Presenter:  DAWSON, Lon (Sandia National Laboratories)

Track Classification:  CC: Establishing and formalizing nuclear security processes into integrated management systems
Executive Summary:
The Technical meeting on advancing maintenance and calibration of radiation detection equipment for nuclear security systems was hosted by the Government of Burkina Faso in conjunction with International Atomic Energy Agency (IAEA) from 6-9th of May, 2019, at Ouagadougou Burkina Faso. Twenty one participants were selected from 11 countries and three experts with wealth of experiences from IAEA were in attendance to share great experiences in maintenance, repair, and calibration of radiation detection equipment for nuclear security. The Countries represented are Nigeria, Senegal, Mali, Ghana, Cameroun, Democratic Republic of Congo, Sierra Leone, Benin Republic, Mauritania and the host, Burkina Faso. The Experts from IAEA are Tyrone Harris IAEA Vienna, Brian Tucker Pacific Northwest National Laboratory (PNNL) USA and Yavor Andreev THETA CONSULT Ltd, Bulgaria.
The technical meeting was designed with the main objective to work with participant to share best practices in maintenance, repair, and calibration of radiation detection equipment for nuclear security. The meeting identified and discussed common issues as regards to maintenance, repair, and calibration needs where science and technology can improve the effectiveness, efficiency, and sustainability of radiation detection systems for nuclear security.

Outcomes: The outcomes of the technical meeting include:
Knowledgeable radiation detection equipment users, maintainers, and specifiers that can improve the maintenance and repair of radiation detection equipment;
Identification of science and technology projects and participants to address detection equipment for nuclear security challenges;
Make some recommendations to manufacturer of radiation detection systems with the aim of improving their operation and maintainability.
Agreements between the participants to work together and/or separately on various projects related to the Technical Meeting on Advancing Maintenance and Calibration of Radiation Detection Equipment for Nuclear Security Systems. Each project have a notional timeline. A report was created after the technical meeting that summarizes the future projects, plans, and needs that were identified during the technical meeting;

Furthermore, participants discussed extensively and proffered professional solutions to issues and challenges raised by member states in attendance at the technical meeting that affects operation, maintenance and calibration of radiation detection equipment for nuclear security systems. Proposals were also made for projects that will offer workable solutions to identified issues and challenges which could further generate an implementable report for the IAEA.
Gender

Male

Primary author:  Mr INYANDA, AROME
Presenter:  Mr INYANDA, AROME

Track Classification:  CC: Advances in nuclear security research and development; international cooperation on nuclear security research
How to communicate Nuclear Security with the Public

As the IAEA declares, “excellence in operations and excellence in communications are mutually reinforcing concepts”. The main objective of this paper is to analyze the impact of communication tools in the nuclear sector. Particularly, we would like to narrate the experience of Argentina in management of security events.

Our main argument states that communication must be considered as a tool that is as relevant as any other, regarding the administration of a nuclear facility. By communication we understand the way in which we address with employees inside power plants or atomic centers, the dialogue with local and national authorities, the interaction of different agencies involved, and, mainly, the way we talk to the society. If this aspect is not taken into consideration, the nuclear sector becomes vulnerable to misinformation.

The Argentine Undersecretary of Nuclear Energy has been working on the improvement of communicational capacities and best practices in security events, as to train and update employees, civil sector and the community in new abilities and mechanisms that will maximize the general output in front of possible incidents. Throughout the recount of a particular local case, we will expose the different and consequent phases communication undergoes, with the agencies involved in the security events and with local community itself.

Finally, we expose actions and recommendations that we believe must be carried out as to transform nuclear topics into more handy themes for the surrounding community, and with more clear and practical rules for the ones that form part of the industry. Regarding the case of Argentina, we will describe the way in which this modifications can be carried out, and in the same way, expose the challenges that may arise.

State

Argentina

Gender

Male

Primary authors: Mr FOURCADE, Martin (Undersecretariat of Nuclear Energy); CÁCERES, L Federico (Undersecretariat of Nuclear Energy); Mr LONGO, P. Matias (Undersecretariat of Nuclear Energy)

Presenter: Mr FOURCADE, Martin (Undersecretariat of Nuclear Energy)

Track Classification: MORC: Coordinated response to nuclear security events
In the last few years, distributed ledger technology (widely recognized in the form of blockchain) has demonstrated practical benefits beyond the development and exchange of cryptocurrencies. Blockchain solutions are being implemented in the fields of international development, healthcare, and education, predominantly as an information-sharing platform that enable parties to interact in a trusted environment. The strength of blockchain stems from its cryptographically-secure properties: when data is recorded onto the blockchain by any user, it is automatically copied onto other connected nodes (or participants) on the chain, as opposed to storing it directly into a centralized database. Consequently, the information has “no single point of failure” in a blockchain; any changes to the information – an attempt to extract or manipulate sensitive data, for instance – will be logged.

Thus, blockchain’s ability to preserve the integrity of data could potentially help enhance security measures across businesses, including the nuclear sector. For instance, blockchain technology could make it difficult for a malevolent actor to reconfigure files or install code that could linger in a computer network undetected, among other applications. This paper outlines the exploratory research the Stimson Center conducted in the Fall of 2019 – including expert interviews with blockchain developers and nuclear facility operators – to better understand the possible applications for nuclear security. The paper examines use cases that could potentially prevent or mitigate security vulnerabilities in nuclear facilities that could be exploited by cyber and insider threats. Moreover, the paper discusses potential difficulties in applying blockchain for nuclear security, and the ways in which the use of this technology could alter security considerations – for better or worse – at the national and operational level.
Track Classification: CC: Information and computer security considerations for nuclear security
One challenge of the risk management process for cyber security within nuclear facilities is understanding how to create scenarios to test deployed security controls that are representative of how threat actors operate. The challenge to creating these scenarios is centered on three issues. First, the complexity of systems and components (assets) at nuclear facilities makes for an expansive attack surface, so the number of viable attack pathways is difficult to approach with any confidence. Second, the nature of cyber-attacks and cyber-campaigns has evolved to include cyber-enabled physical attacks and physical-enabled cyber-attacks, which blends together attack types which have traditionally been treated separately. Third, threat actor capabilities vary depending upon the resources they have available to them and their domain experience. Our paper provides for a methodology to create blended threat nuclear-cyber scenarios for use during research, assessments, and exercises in support of risk management and training objectives.

Our methodology was derived through a series of International Atomic Energy Agency (IAEA) consultancy series and a multi-year research project on detecting events within nuclear facilities that may indicate that a cyber-attack is taking place. The first step in our methodology was to agree upon an attack and defense framework that would allow us to describe each scenario in a common way. This normalized scenario development vocabulary is critical for adoption. The next step was to choose an approach to representing the tactics and techniques used by cyber actors (both attackers and defenders) and so we integrated the MITRE ATT&CK model into our scenario development process. This vocabulary is abstractly represented such that both cyber and physical attacks can be represented across a common attack and defense framework. The third step in our methodology was to develop a series of interactions that would be created using the framework objects as defined. The last step of the methodology was to provide reference implementations for research, field assessments, and exercises such that specific threat actor capabilities can be layered on top of each step of the methodology.
Track Classification: CC: Information and computer security considerations for nuclear security
Consequence-driven Cyber-Informed Engineering

Cyber Informed Engineering (CIE) was defined in IAEA CN-244-520 as the inclusion of the cyber-attack and defense perspective (cyber security aspects) into the engineering process. It is the process by which engineering personnel are made aware of how their current actions impact the processes by which they architect and design systems. Decisions do not always take into consideration the attack tactics, techniques and procedures currently in use by capable cyber-adversaries. Consequence analysis and associated engineering mitigations are some of the most important elements within the CIE framework. Ensuring the most critical functions are available to perform as designed, when called upon, is vital. Idaho National Laboratory (INL) has created an operational process for performing cyber-informed consequence analysis and engineering mitigations. Consequence-driven Cyber-informed Engineering (CCE) is a cyber defense concept that focuses on the highest consequence events from an engineering perspective so that resource-constrained organizations receive the greatest return on their security investments. The CCE process helps nuclear asset owners to: identify high-impact / high-consequence events that could result in interruption of critical functions, analyze the infrastructure which could be subverted to enable those events, and develop specific mitigations to avoid, or engineer out, these consequences. An operational approach to CCE is provided.

State
United States

Gender
Male

Primary authors: ANDERSON, Robert (Idaho National Laboratory); SMITH, Robert (Idaho National Laboratory)

Presenter: ANDERSON, Robert (Idaho National Laboratory)

Track Classification: CC: Information and computer security considerations for nuclear security
Cyber Security Considerations for Implementing the Design Basis Threat at Nuclear Facilities

Cybersecurity threats continue to grow, and the nuclear sector recognizes that it must have compensating measures in place to address these threats. The evolution of cyber threats to critical systems is growing at an alarming rate and it is important that the nuclear community response accordingly. One mechanism to addresses the cyber threat is through development and utilization of a Design Basis Threat (DBT). Historically the DBT was originated as a key element in a toolset enabling an Operator to gain a physical security perspective based on understanding the capabilities of an adversary to cause acts of radiological sabotage or the theft of special nuclear materials.

The DBT enables the Operator to implement a baseline protective strategy required by the State. The DBT outlines the threat adversary’s capabilities. Motivations and Opportunities are further informed by the Intelligence Partners, and the Operator’s Defensive Strategy and Posture. This guidance allows the Operator to develop the necessary site security plan and protection systems to meet the DBT requirements.

The purpose of this paper is to outline how cyber security DBT considerations can impact the physical security protective strategy and provide a methodology for operators and competent authorities to utilize to ensure that the DBT is integrated into the cyber mitigation strategies both from the cyber-physical perspective as well as the physical-cyber perspective. The dynamic nature of the threat based on day-to-day changes that occur in cyber security – vulnerability discovery and mitigations - directly affects the DBT model review and update cycle by the CA and Operator evaluation and implementation.

A nuclear security framework that supports the DBT requirements as well as the security challenges must be considered within the site-specific nuclear security plan that is approved by the component authority. The approach will very state to state, from very prescriptive measures to simple self-directed security implementations subject to an occasional compliance-based assessment. Therefore, this paper will evaluate the cybersecurity challenges associated with creating, managing and utilizing a DBT by examining the physical and cybersecurity protective measures developed through a risk-based assessment process, within the context of what is required by the competent authority to promulgate and support the Operator’s appropriate protection profile to prevent the theft or sabotage of nuclear materials.

State
United States

Gender
Male

Primary authors: RODRIGUEZ, Julio (Idaho National Laboratory); Mr KNIGHT, Jeffrey (Idaho National Laboratory)

Presenter: RODRIGUEZ, Julio (Idaho National Laboratory)
Track Classification: CC: Information and computer security considerations for nuclear security
Enabling Multicultural Exchange on International Technical Research Projects

In the summer of 2016, the International Atomic Energy Agency (IAEA) launched a Coordinated Research Project (CRP) on Enhancing Computer Security Incident Analysis at Nuclear Facilities (J02008). The primary objective of this CRP was to improve computer security capabilities at nuclear facilities to support the prevention and detection of, and response to, computer security incidents that have the potential to either directly or indirectly adversely affect nuclear safety and nuclear security. The secondary objective was to establish an international community of experts to facilitate the exchange of good practices in the field of computer security incident response at nuclear facilities. [a] The fields of nuclear security and nuclear nonproliferation have a long history of multinational problem solving. The field of cyber security has not enjoyed this same history as meaningful collaboration in this field requires disclosure of vulnerabilities and weaknesses. Add to this geo-political conflict in the cyber domain at the nation state level and bringing together nations to work collaboratively on this type of project was sure to experience a unique set of challenges.

This paper describes the confidence building processes that occurred over the course of the past three years between the CRP participants from the countries of: Argentina, Brazil, Canada, China, Germany, Ghana, Hungary, Mexico, Pakistan, Poland, Republic of Korea, and the United States of America. Our findings illustrate a few interesting processes where well-resourced cyber-capable nations have to adjust their approach to accommodate nations still growing their capabilities. We observed how contributions from narrowly focused research teams could be incorporated into a testbed while broad frameworks could be constrained to allow for varying levels of model fidelity. We feel the most significant observations are of how relationships were formed and developed to allow for meaningful multicultural exchange. We hope that our findings will help future nuclear-cyber projects to structure themselves in such a way as to decrease the time it takes for parties to trust each other and thus bring the joint-research capability to fruition in short time.

State
United States

Gender
Male

Primary authors:  HEWES, Mitchell (IAEA); SPIRITO, Christopher (Idaho National Laboratory)

Presenters:  HEWES, Mitchell (IAEA); SPIRITO, Christopher (Idaho National Laboratory)

Track Classification:  CC: Information and computer security considerations for nuclear security
Computer Security & Threat Analysis: Minimizing The Attack Surface

Nuclear and radiological facilities are digitizing elements of security and operational systems in order to improve performance, effectiveness and efficiency while reducing cost of ownership. These digital elements have greatly increased the interconnectivity between traditionally disparate systems such as components in physical protection systems (PPS), nuclear material control & accounting systems (NMAC), as well as other security and operational systems at a nuclear power plant. The migration to digital technology, along with the increased interconnectivity, has introduced new vulnerabilities. These vulnerabilities, which may go unobserved and undetected, present a new landscape of opportunity for potential threat actors targeting nuclear and radiological facilities.

Recent advances in adversarial modeling have generated new and valuable perspectives on existing and emerging threat characteristics, capabilities, and potential attack vectors. The models identify elevated security risks of a threat actor incorporating cyber based attack tools into theft and sabotage scenarios. The risks are particularly pronounced for insider threats that can leverage legitimate access and authorized privileges to conduct maloperations and/or introduce malware to achieve attack scenario goals.

There is a demand from member states and global subjective matter experts for actionable intelligence that can help define accurate prescriptive measures related to how cyber security guidance should be implemented. The landscape of referenceable case studies specific to cyber / physical attacks on nuclear instrumentation and control is poorly populated even though there is an abundance of information on both general non-nuclear cyber security events and physical attack methods.

To address this need, researchers selected actual cyber security attack methods and fused them with well-known insider and physical attack trends. As a result, plausible attack use cases were developed to demonstrate how after-action analysis can be performed to define how a threat actor could use combined cyber/physical methods to accomplish their goal of creating a nuclear reportable event. The goal being to create use cases applicable to the nuclear industry. The presentation will include analysis of cyber event investigation, artifact analysis, attack tree modeling and a comprehensive discussion on how NSS 33-T can be used to proactively defend against the adversarial methods and tactics illustrated in the use cases.

State
United States

Gender
Male

Primary authors: FABRO, MARK (LOFTY PERCH); NICKERSON, Charles (Idaho National Laboratory)
Presenters: FABRO, MARK (LOFTY PERCH); NICKERSON, Charles (Idaho National Laboratory)

Track Classification: CC: Information and computer security considerations for nuclear security
Assistance for Enhancing Nuclear and Radiological Security: Beyond the IAEA Alone

Many States need and have requested assistance to implement their national nuclear and radiological security objectives, especially their obligations under a range of legally binding international nonproliferation instruments. The International Atomic Energy Agency (IAEA) has a host of technical assistance programs to meet many of those needs, and an extensive record of providing such assistance. Unfortunately, persistent gaps in implementation, such as those identified in the 2016 Comprehensive Review of the UN Security Council resolution 1540 (2004), indicate that despite the IAEA’s good work, the need for assistance has not abated.

Clearly, the International Atomic Energy Agency (IAEA) has the central and most important role in providing and, where appropriate, coordinating these assistance activities. At the same time, many other entities have made important contributions to assistance in the realm of nuclear and radiological security, perhaps best recognized in the 2016 Nuclear Security Summit Action Plans with the United Nations, INTERPOL, the Global Initiative to Combat Nuclear Terrorism and the Global Partnership against the Spread of Weapons of Mass Destruction, as well as the Action Plan with the IAEA. Until now, however, no exploration of the work by other entities could draw on a comprehensive database of relevant assistance activities. With funding from the Canadian Department of Foreign Affairs, Trade and Development (DFTAD), however, the Stimson Center has recently developed a searchable, open source, online database of more than 1500 WMD nonproliferation assistance programs and projects (available at https://1540assistance.stimson.org).

A preliminary analysis of the more than 400 entries in the database directly associated with either radiological or nuclear security indicates that many dozens of other entities participate as assistance funders or providers in the process. As important, an even larger number of entities serve as implementers, connecting those providing and those seeking assistance. In this paper, after a brief review of the extant coordination mechanisms for nuclear and radiological security assistance, the author will explore the scope and scale of the assistance contributions made by other international bodies, States, academic institutions, civil society organizations, and foundations, along with those of the IAEA. The paper will cover, for example, what types of assistance these organizations provide, the geographic location of their activities, and the relationship between the providers or funders of assistance programs and the implementers of the activities. The author will also explore how well these programs match needs expressed by UN Member States through requests for assistance to the Committee established pursuant to UN Security Council resolution 1540 (2004) and through requests for assistance expressed in national statements by IAEA members during the last five General Conferences. The author also will explore some of the challenges States face in requesting and securing assistance and generate some hypotheses for future research. To conclude, the author will use the findings to generate several recommendations on how the international community can enhance their efforts to assist States in meeting their nuclear and radiological security objectives, thereby contributing to increased international peace and security.

State

United States

Gender
Male

**Primary author:** Dr CUPITT, Richard (Stimson Center)

**Presenter:** Dr CUPITT, Richard (Stimson Center)

**Track Classification:** MORC: The IAEA’s technical support for States that takes into consideration complex threats and challenges including geographical condition
Impact of IoT (Internet of Things) on traditional Insider Threat Mitigation

Traditionally, nuclear Insider Threat programs have focused upon those individuals with trusted access to facilities and or sensitive information, the abuse of which could lead to unacceptable consequences. Prior to the advent of digital technology, “insider threat” was usually limited to physical attacks focused on theft or sabotage. Recent integration of remote connectivity, engineering support, integrated sensor networks and maintenance contracts have led to critical environments existing within and often dependent upon a complex web of constant communication. While this construct enables employees and trusted third parties to more effectively monitor and operate nuclear related processes, it also places a strain on traditional definitions of “Insider Threat” and requires consideration of both “Unwitting Insiders”, those whose actions enable a cyber attack without their intent, and “Unknowing Insiders” or cyber mules who’s compromised devices or accounts enable a malicious actor without their knowledge.

Against this backdrop of emerging insider challenges cyber programs have stepped up to address both the intentional cyber insider and the unknowing/unwitting participants. New programs educate the user on proper use of computers and applications, the threat of phishing emails and have implemented the use of mandatory kiosks to validate digital media prior to deployment in sensitive areas. This is all productive and worthwhile, but the new wave of Internet of Things, (IoT) creates even more nuanced cyber threats and a very real scenario in which the user themselves represent a walking digital asset and may not in fact even realize the potential that they create for abuse as a cyber insider.

This presentation looks at where insider threat mitigation is today, how the models differ from a person to person perspective vs within the computing world, especially that of critical systems automation, and where it will be in the near future as implanted medical devices, wearable technology and even Elon Musk’s “Neural link” become the norm and the ability to identify “Cyber Insiders” ceases to have any relevant meaning with regard to cyber threat mitigation.

State
United States

Gender
Male

Primary author:  HOFFMAN, Rob (Idaho National lab, USA)
Presenter:  HOFFMAN, Rob (Idaho National lab, USA)

Track Classification:  CC: Information and computer security considerations for nuclear security
Challenges of maintaining the security of radioactive sources of categories 1, 2, and 3 in case of abnormal conditions

KAMAL H. LATEEF  
Iraqi Radioactive Sources Regulatory Authority  
Baghdad Iraq  
Chairman@irsra.gov.iq

FADHIL H. MIZBAN  
Iraqi Radioactive Sources Regulatory Authority  
Baghdad Iraq  
fadhil_res@irsra.gov.iq

Abstract

The security of radioactive sources, nuclear materials and the facilities they contain is related to the provision of factors related to the human role, while others are related to the technical aspect in a way that provides the following security elements: deterrence, detection, delay, response and security management. The human role represents the administrative procedures which consist of monitoring, guards, alarms evaluation and conversion to declaration of detection status followed by disability and delay to provide the necessary time to respond and security management. An important part of the deterrence concerns the human role. The presence of specific location can provide sufficient deterrence. The assessment of alarms is carried out through a human element, up to the announcement of a detection situation. The work of disability and response is carried out by the human role to a large extent. This task cannot be accomplished without the human role. In the same context, the technical factors require activation to be provided to the main and alternative sources of energy, as the means of deterrence and detection (cameras, sensors of movement, padlock, etc.) all require continuous supply of electrical energy and the loss of energy sources eliminates the full existence of the technical role. The integration of the work of technical and human role is required to be carried out within the framework of a comprehensive security system or community stability in general. The occurrence of abnormal events such as loss of state control and the collapse of the system, the occurrence of severe environmental disaster or the occurrence of wide range military operations that would lead to the loss of the human role or leads to loss of technical role as well. Which is happening in the city of Mosul where the selection of ISIS gangs calling for the medical complex as an area of operations led to the medical complex to the consequences and severe damage to buildings, electrical power supply and infrastructure, which led to the loss of the human and technical role, thus the loss of all elements of security elements (deterrence, detection, delay and impediment, response and security management), Unauthorized access to the therapeutic source (the cobalt-60 unit) had happened and fortunately the unauthorized arrivals were thieves who were looking for any simple material theft so they stealing electrical connections and some operation components of the device, so can be imagine the sabotage scenario if the adversary are terrorists and they have the capability and intention, with presence of attractiveness, and ease to access to the radioactive source, by making a simple threat assessment, according to practical information regarding to the security situation and terrorist capabilities, the conclude is
threat assessment rating is very high. In order to prepare for such situations, the role of the technical factor should be greater and work independently of the human role, such as providing teletherapy treatment rooms or any rooms containing high-level radioactive sources from first or second categories with automatic doors operated by an independent power supply and closed in special cases such as earthquakes, explosions, war operations, hurricanes and floods, or if they are activated by the security official when they feel that a certain danger is imminent. The opening of these doors should be difficult without special codes that are equipped exclusively for those authorized person.

**State**

Iraq

**Gender**

Male

**Primary author:** Dr LATEEF, Kamal (Iraqi)

**Co-author:** Mr MIZBAN, Fadhil (Iraqi)

**Presenter:** Mr MIZBAN, Fadhil (Iraqi)

**Session Classification:** Physical protection systems: evaluation and assessment

**Track Classification:** PP: Physical protection systems: evaluation and assessment
Criticality Safety and Security Interface for Nuclear Materials Related to a Research Reactor

The fundamental interface between nuclear safety and security is to protect and prevent the harmful effects of radiological hazards, also detect the unauthorized access, sabotage and illegal transfer or other malicious acts involving nuclear materials and radioactive substances.

Safety and security cultures aren’t opposing each other but mutually reinforce one another with complementary. Nuclear security fundamentals should be applied and managed by the operating organization to achieve the regulatory requirements related to the interface between safety and security.

The interface between safety and security for a research reactor should be implemented in an integrated manner throughout the lifetime of the reactor. Safety measures and security measures shall be established in such a way that they do not comprise one another.

In this paper we will deal with the nuclear material exists in the site boundary of a research reactor to achieve its security, criticality safety in the reactor core and sub-criticality in other storages for the spent fuel or for the fresh fuel. Also, the interfaces between safety and security during the handling, manipulation, transfer, operation and long-term storage of the nuclear materials should be defined.

Nuclear materials in a reactor site can be categorized as;

- Nuclear fuel in the reactor core;
- Fresh nuclear fuel in the fresh fuel storage;
- Fresh nuclear fuel targets contain LEU in the fresh target storage;
- Irradiated LEU fuel targets; and
- Irradiated nuclear fuel in spent fuel storage.

The safety and security for these nuclear materials should be managed by the operating organization and supervised by the regulatory authority based on the IAEA Safety Standards and Code of Conduct for the Safety of Research Reactors.

Also, the criticality safety for the nuclear fuel in the reactor core should be modeled and calculated at each new core configuration or fuel loading to avoid over excess reactivity and achieving the Operational Limits and Conditions (OLCs).

The Criticality safety calculations for the fresh fuel storage, fresh LEU targets storage and for the spent fuel storage should achieve the sub-criticality in all operational states.

Moreover, the calculation of the radionuclides and source term of the spent fuel to determine the amount of plutonium produced, amount of uranium consumed, and amount of fission products contained will be considered and modeled. The spent fuel inventory and source term characterization and the radiation activity are necessary for the safe long-term storage of spent fuel, safeguards control, fuel transport for reprocessing or in case of nuclear accidents or theft states of the nuclear spent fuel. These information assist in the nuclear material categorization which can assist for specifying appropriate physical protection measures against unauthorized removal of nuclear material.

The concept of defense in depth in nuclear material transport for the preventive and protective measures for the protection of nuclear material will be presented. The defense in depth should be incorporated in the design of the physical protection system to provide the function of detection, delay, and response. Each function should be provided by multiple independent measures. There are requirements should be established for protecting the confidentiality of sensitive information.
relating to the transport of nuclear material. The information include the schedule, the route, shipper, carriers, and means of the transport or the waiting station.

The role of regulatory authority for the security requirements, and the methods of out-of-core measurement systems to measure gamma or neutron emissions from the nuclear fuel assemblies will be highlighted.

The IAEA activities towards the interface between safety and security, nuclear material accountability, malicious acts, physical protection and upgrading of the security systems will be presented. Also, the methods of maximizing the synergy between safety and security for a research reactor from the beginning of the reactor design will be addressed.

**State**

Egypt

**Gender**

Female

**Primary author:** Dr ABOUALO, Rowayda (Lecturer)

**Presenter:** Dr ABOUALO, Rowayda (Lecturer)

**Track Classification:** CC: Nuclear safety and security interfaces
Toward Radiation Detection Sustainability: Failure Analysis and Life-cycle Cost Estimation in Burkina Faso

In order to detect nuclear and other radioactive material, mitigate and combat illicit trafficking, illegal transport and any other unauthorized or malicious acts, countries deploy usually detection equipment within and at their borders. Most of the non-advanced countries focuses their detection systems on handheld equipment. The main issue after deployment of detection equipment is to make this system sustainable and effective.

Indeed, breakdown could occur at inappropriate time leading to the failure or interruption of the detection system and increasing the chances of malicious or unauthorized acts.

The common failures recorded from different countries in particular from Burkina Faso are inter alia damage to cables, break of handle, and probe, loss of cables, short circuit in charging transformer, break or wear of connectors and pins, leakage of batteries, software corruption and outdate, etc.

The failures are due to manufacturing features (robustness, resistance), human factor (negligence, misuse) and drastic environment effect (Temperature, humidity, dust).

Another important issue is calibration of detection instrument, ensuring they are working properly and detecting efficiently. In general, most of manufacturer recommend to calibrate instrument once a year unless the country has its own regulation.

The cost for maintenance of equipment, including repair, calibrating periodically in a referred laboratory or at manufacturer side, replacement and spares, seems too high for non-advanced countries.

This study is from a part of research project under the J02012 Coordinate Research Project (CRP) on Advancing Radiation Detection Equipment for Detecting Nuclear and Other Radioactive Material Outside of Regulatory Control. To achieve ultimate goal of the CRP to improving efficiency of the equipment and sustaining detection systems, it is crucial to understand causes and rates of failures to be able to manage maintenance and calibration plan to sustain the systems. Therefore, this study aims to analyse failure rates, and estimating life-cycle cost of radiation detection systems for Nuclear Security in Burkina Faso. Forecasting the cost of maintenance could help to avoid the inoperability of detection systems due to the lack of funds to repair, calibrate or replace the equipment when needed.

Proceeding by failures analysis and rate calculation, this work allowed to: (i) assess the operability (reliability, maintainability and availability) of the detection system for the country; (ii) assess the life expectancy for a given instrument; (iii) estimate the cost of maintenance based on different scenarios and alternatives.

The benefit of such approach is to master the expenses linked to detections instruments and their lifecycle maintenance.

In the case of Burkina Faso, taking into account different alternative to maintenance, mainly calibration, the initial planned cost of maintenance which was too high, has been reduced by 64%.

But this suggest the validation and approval of some internal calibration procedures using standard sources and determining correction factor. These internal methods may help to reduce resorting systematically to standard laboratory for calibration.

In addition to this alternative, a comprehensive management system for maintenance of the overall detection system as well as human resource development programme based on identified weaknesses and training needs, also contribute a lot to reducing the lifecycle cost.

State

Burkina Faso
Gender

Male

Primary authors:  Mr NABAYAOGO, Delwendé (National Authority for Radiation Protection and Nuclear Safety);  Mr ZOUNGRANA, Martial (National Authority for Radiation Protection and Nuclear Safety)

Presenter:  Mr NABAYAOGO, Delwendé (National Authority for Radiation Protection and Nuclear Safety)

Track Classification:  MORC: Detection technology development and performance testing
Nuclear Material Accounting & Control (NMAC) for Practitioners: A New Approach to International Training on NMAC Concepts

In August 2018, the Nuclear Security Division of the International Atomic Energy Agency (IAEA) presented the first-ever pilot International Training Course (ITC) on “Nuclear Material Accounting & Control (NMAC) for Practitioners” in conjunction with the United State Department of Energy/National Nuclear Security Administration Office of International Nuclear Security (NA-21.1) and Los Alamos National Laboratory (LANL). The course was truly an international event, with twenty-four participants from over fifteen nations as well as instructors from another half-dozen countries. The course curriculum, based on IAEA Nuclear Security Series No. 25-G, Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities, was developed collaboratively with experts from a dozen countries worldwide contributing their knowledge and experience to enhance the material with real-world examples. Subjects covered included the interplay between NMAC and other elements of nuclear security, including information and cyber security; records and procedures; physical inventory taking, material-unaccounted-for (MUF) evaluation; nuclear material measurements; measurement quality control; controls, including tamper indicating devices (TIDs) and item and process monitoring; resolution of irregularities; and performance testing. With the IAEA NMAC implementing guide 25-G providing the overarching framework, the course provided the opportunity for “deep dives” into key topics of operational interest to NMAC practitioners, such as the evaluation of measurement control data and proper selection of controls for various facility types. Another key goal of this course, with its emphasis on practitioners, was to provide hands-on experience and opportunities for nuclear material measurement and implementation of controls. This was met with over thirty percent of the two-week course spent in the laboratory, working with nuclear material standards available at LANL. The course culminated in a day-long capstone exercise which served as a final integrated test, putting to work the material covered in the preceding weeks. During the capstone exercise, the participants were afforded the opportunity to conduct a nuclear material inventory, apply and remove TIDs; use procedures tailored to the scenarios; make nuclear material measurements; investigate and resolve irregularities that were planted in the scenario; and report to relevant authorities. Feedback from the participants was extremely positive, with great benefit realized by the ability to incorporate the concepts being taught into an authentic environment. The hands-on component was recognized as extremely valuable, providing concrete benefits for the participants to take back to their home facilities. The addition of a hands-on, advanced International Training Course in NMAC specially tailored to practitioners from nuclear facilities worldwide contributes substantially to strengthening the nuclear security regime, and represents an outstanding addition to the IAEA’s flagship courses in nuclear security.
**Primary authors:** Ms MARLOW, Johnna (Los Alamos National Laboratory); Mr LARSEN, Robert (International Atomic Energy Agency); Ms BROWNELL, Lorilee (U.S. Department of Energy, National Nuclear Security Administration)

**Presenter:** Ms MARLOW, Johnna (Los Alamos National Laboratory)

**Track Classification:** PP: Nuclear material accounting and control
China’s Follow-up Actions of the International Physical Protection Advisory Service (IPPAS) Mission

The International Physical Protection Advisory Service (IPPAS) of the International Atomic Energy Agency (IAEA) is an essential part of IAEA’s efforts to assist Member States to establish and maintain an effective nuclear security regime. Upon the request of the Government of People’s Republic of China, IAEA conducted the IPPAS mission in China from 28 August to 8 September 2017. During this mission, the IPPAS experts team reviewed China’s national nuclear security regime for nuclear material and nuclear facilities, and assessed the physical protection technical measures and management procedures at Fangjiashan-1 Nuclear Power Plant, Qinshan Nuclear Power Base. Through the IPPAS mission, a number of recommendations, suggestions and good practices were identified, which covered the aspects of legislation, regulatory, human resource development, nuclear security culture cultivation, performance evaluation, etc.

Following the recommendations and suggestions given by IPPAS experts team, China Atomic Energy Authority (CAEA) as the competent authority of nuclear industry management, has taken a series of follow-up actions to furtherly strengthen the nuclear security regime. The progress of legislation regarding nuclear security was accelerated significantly. A lot of departmental rules and technical guidance more aligned to CPPNME were developed and went into effect. The investment in nuclear security capacity building was increased continuously. The nuclear security culture and awareness were obviously improved both on managerial and operational levels through a set of systematic and large-scale trainings. The technical measures protecting nuclear materials and facilities against various of emerging nuclear security were constantly upgraded and enhanced.

With the lessons learned from IPPAS mission, China is engaged in developing a comprehensive mechanism of performance testing and evaluation for nuclear security systems, measures and staffs. For example, conducting performance testing for nuclear security system and equipment in their design, installation and operation phases; performing peer reviews on physical protection system effectiveness and nuclear security culture sustainability, normalizing the force-on-force exercises on nuclear security events response at nuclear facilities, etc.

This article will give a brief introduction to the follow-up actions taken by CAEA for the IPPAS mission. The archived progress and results of these actions will be evaluated, and their effects on the sustainable development of nuclear security in China. We believe the practices and experiences learned by China should also be benefitted for other member states to recognize the importance of IPPAS mission in improving their nuclear security capabilities and maintaining a more effective nuclear security regime.
Center)

**Presenter:** Mr GU, Shaogang (State Nuclear Security Technology Center)

**Track Classification:** PP: International Physical Protection Advisory Service: good practices and lessons learned
SNSTC’s Capabilities and Practices on Performance Testing for Nuclear Security System and Equipment

The State Nuclear Security Technology Center (SNSTC) was established with the approval of the Chinese central government in November 2011. As an affiliate to China Atomic Energy Authority (CAEA), SNSTC’s primary mission is to provide technical support for the government management on nuclear security, nuclear materials control, nuclear export & import control and nonproliferation; and to conduct international exchanges and cooperation. SNSTC is also the operator of China’s Center of Excellence (COE) on Nuclear Security. Since the operation of COE in March 2016, SNSTC has received the ISO-9001:2015 QMS certificate and its laboratories have been certified by China National Accreditation Service for Conformity and Assessment (CNAS) and China Metrology Accreditation (CMA) in 2017. With the comprehensive testing capabilities on function/performance, environmental applicability and electromagnetic compatibility for nuclear security related system and equipment, SNSTC has completed more than 450 tests for about 100 sets of radiation detection and physical protection equipment for nuclear facilities, customs, universities and other relevant stakeholders.

As a third-party testing agency, SNSTC was commissioned by General Administration of China Customs to take performance testing and acceptance testing for the radiation portal monitors to be deployed at border ports in 2017-2018. The testing included 46 test items, covered the various aspects such as radiation detection function, radiation detection performance, environmental adaptability, electromagnetic compatibility and long-term reliability, etc. In addition, SNSTC led the technical review and in-field acceptance testing for several physical protection system upgrading projects in China, and conducted the physical protection system effectiveness evaluations for many times as requested by nuclear facility operators. Based on the works above mentioned, SNSTC also developed a series of technical documents, such as the Management Measures on Acceptance of Physical Protection Engineering, the Technical Guidance on Acceptance Test of Physical Protection System in Nuclear Facilities, the Technical Specifications for Central Control Room of Physical Protection System in Nuclear Facilities, the Technical Specifications of Digital Radiation Imaging Device used for Vehicle Access Control in Nuclear Facilities and so on.

This article will provide a briefing introduction to SNSTC’s capabilities and practices on performance testing for nuclear security related systems and equipment. Some typical cases on performance testing in lab and field conditions for radiation detection equipment and physical protection systems should be demonstrated. The general objects, procedures and requirements of performance testing should be introduced. Furthermore, the necessity of and lessons-learned from performance testing, and its importance for nuclear security sustainability on national and facility levels should be discussed.

State

China

Gender

Female
Primary authors: Ms WANG, Shuo (State Nuclear Security Technology Center); Mr GU, Shao-gang (State Nuclear Security Technology Center); Mr YANG, Changjie (SNSTC); Mr HAN, Yeliang (SNSTC)

Presenter: Ms WANG, Shuo (State Nuclear Security Technology Center)

Track Classification: MORC: Detection technology development and performance testing
Graphene fiber for the personal protection, and mitigating the nuclear and radiological accident consequences

Radioactive material dispersion and attacking nuclear facilities could be used for terrorism or other criminal acts. These incidents would lead to serious consequences such as human health and environment damage, creating panic, and affecting economic and political stability. Since 1993 to 31 December 2018, ITDB shows a total of 3497 incidents of unauthorized activities and events involving nuclear and other radioactive material, where 285 incidents were related to the illicit trafficking or malicious use [1]. These incidents lead to concerns of a possible radiological or nuclear terrorist attack.

Radiological terrorism using radiological dispersal device (RDD) is more likely to occur due to the relatively large number of commercially used radioactive materials and hundreds of nuclear facilities worldwide. With the increasing possibility of these incidents, the necessity of effective radionuclide adsorbing material is increased for the personal protection of the first responder as well as cleaning up radioactive materials and decontamination of buildings.

Graphene fiber could ensure the protection against gaseous radioactive elements and various chemical agents through the adsorption. Graphene-based materials have several benefits over currently used activated carbon such as large specific surface area up to ~3000 m²/g [2], high chemical/thermal stability, tunable specific surface area and pore structure, relatively low cost and easy scale-up associated with the manufacturing of the porous graphene carbons [3]. The high specific surface area of the graphene fiber increases the adsorption capacity. Different functionalized graphene fiber also could be capable to selectively adsorb different radioactive gases at various levels of relative humidity and conditions.

Various studies on graphene-based materials demonstrated the potential opportunities of graphene fiber for the use of personal protection through the adsorption of gaseous toxic elements. Anna Yu et.al shows the interaction of GO with actinides including Am (III), Th(IV), Pu(IV), Np(V), U(VI) and typical fission products Sr(II), Eu(III) and Tc(VII), along with their sorption kinetics [4]. Higher sorption affinity towards the toxic elements from different solution makes graphene oxide a promising new material for the radioactive nuclide removal and containment. Graphene-enhanced composite material GO/amidoxime hydrogel (AGH) shows the selective removal of uranium from aqueous solutions [5]. In the case of CO₂, H₂, CH₄ adsorption, the performance of graphene-based adsorbents is often higher, especially at high pressure [2][3]. Also, Graphene-based materials have potential opportunities for nuclear decommissioning [6].

This paper presents the effectiveness of graphene fiber as a potential sorbent of iodine (I₂(g)). Also, the performance of silver functionalized graphene fiber is investigated, which would allow more selectively capture of iodine among other different elements. The graphene oxide fibers are produced through the wet spinning process using a coagulation bath of 5wt% CaCl₂ into the solution of ethanol/water (1/3 v/v), which is shown in Fig.1. For the silver functionalized graphene fiber, silver nitrate (AgNO₃) solution is added with the graphene oxide solution. Figure 2 shows the SEM images of the fabricated graphene oxide fiber and Ag functionalized graphene oxide fiber. The graphene fibers are exposed to a saturated iodine environment through the use of a desiccator, in which solid iodine crystals are placed. Iodine uptake is determined by the change in mass of the tested samples before and after exposure to the saturated iodine environment.

References


State

Bangladesh

Gender

Male

Primary authors: Mr RYU, Ho Jin (Associate Professor, Dept. of Nuclear and Quantum Engineering Korea Advanced Institute of Science and Technology); Mr AHMED, Md. Mobasher (Scientific Officer, Center for Research Reactor, AERE, Bangladesh Atomic Energy Commission (BAEC), Dhaka-1000, Bangladesh)

Presenter: Mr AHMED, Md. Mobasher (Scientific Officer, Center for Research Reactor, AERE, Bangladesh Atomic Energy Commission (BAEC), Dhaka-1000, Bangladesh)

Track Classification: CC: Emergency preparedness and response and nuclear security interfaces
SNSTC/COE’s Practice on Human Resource Development in the Field of Nuclear Security

Abstract:
Nuclear security is a shared responsibility of the international community. China claimed political views to build sustainable and balanced global nuclear security framework through stepping up political input, national responsibility, international cooperation and nuclear security culture, which fully demonstrates China’s responsibility to work with other countries to promote global governance of nuclear security. Since Center of Excellence (COE) of China came into operation in 2016, hundreds of training courses and workshops have been held, training more than 3000 professionals for international community. COE are ready to continue to contribute to nuclear security training and human capacity building for the Asia-Pacific region and the world [1].

Background
As of March 31st 2019, China has put into commercial operation of a total of 45 nuclear power units (excluding nuclear power information in Taiwan), with installed capacity of 45895.16 MWe [2]. Chinese government attaches great importance to nuclear security, and has made efforts to enhance the security of nuclear materials and facilities and ensure the sustainability of nuclear security. The State Nuclear Security Technology Center (SNSTC) was established in November 2011. As an affiliate to China Atomic Energy Authority (CAEA), SNSTC’s main function are to provide technical support for nuclear material regulatory, nuclear security and nuclear export & import; to conduct nuclear security international exchange and cooperation; to undertake the construction and operation of COE.
COE was completed and put into operation in March 2016, which was built in cooperation with the United States. COE integrates mature and advanced technology & instruments at home and abroad which cover nuclear security, nuclear safeguards, nuclear material control, physical protection and other fields, including Demo & Training building, Analytical Laboratory, Environmental Laboratory, MOCK facility, Nuclear Material Bunker, Response Force Training and Exercise Facility and Physical Protection Test Area. The center acts as an international platform for nuclear security human resource development, technology R&D, international exchanges, equipment testing and certification [3].

Objective
This paper emphasizes the importance of nuclear security in China, demonstrates that China has attached great importance on nuclear security human resource development, and expresses SNSTC/COE’s great effort and good practices on improving training and human capacity building for domestic and Asia-Pacific region.

Structure
This paper is divided in six sections. The first section introduces overview of SNSTC/COE as the China’s sole comprehensive nuclear security training and R&D organization. The second section provides introduction of essential facility and equipment. The third section explains the unique features of nuclear security training of SNSTC/COE. This explanation will include an in-depth discussion of five constituents: curriculum system, systematic approach to training, instructor identification, training tools, information management. The fourth section reviews output of continuous international cooperation and collaboration between SNSTC/COE and partners. The fifth section describes challenges and the way forward, and the sixth section concludes the paper.

Reference List
State
China

Gender
Male

Primary authors:  Mr CHEN, Chen (State Nuclear Security Technology Center);  Mr LIU, Xin (SNSTC)

Presenter:  Mr CHEN, Chen (State Nuclear Security Technology Center)

Track Classification:  CC: Role of Nuclear Security Support Centers to support and sustain national nuclear security regimes
Certification bodies play an increasingly important role in the NMAC of bulk nuclear facilities in China

In recent years, the threat of international nuclear terrorism is becoming increasingly serious, and the risk of the proliferation and loss of nuclear materials is increasing. In order to ensure the safety of human beings and the international community and prevent nuclear materials being stolen and illegally transferred, effective technology is needed to account and control nuclear materials. The accuracy of nuclear material measurement needs to be evaluated by uncertainty. IAEA has issued 6 international target values for the protection and calculation of nuclear materials so far, namely, 1983, 1987, 1988, 1993, 2000 and 2010. Both the facilities and the inspection agencies need the reference value of the measurement method performance index, which is used to determine the volume, quality or isotopic composition of the measured object. The target value can be used as a reference standard to judge the validity of the measurement.

In production practice, all kinds of errors are superimposed and transmitted each other. In the bulk nuclear facilities, the total error variance is influenced by random error, long term system error and short term system error. In order to make MUF closer to the real value, in accounting, we need to seize the key main error factors, improve the measurement system and the measurement accuracy. The target value includes the random error and the system error. It is necessary to carry out the experiment and data comparison for each material and each method of analysis and measurement to get the effective uncertainty target value. Uranium forms are mainly uranium hexafluoride (depleted, natural, low concentration), natural uranium, low enriched uranium, uranium oxide, uranium metal. Taking the measurement of 235U enrichment as an example, it can be divided into DA and NDA methods. Comparison activities involve many factors such as sample preparation, distribution, transportation of radioactive materials, activity organization and other factors. It will be faced with many challenges in the future.

Especially, there is no very effective scientific method for estimating the holdup in equipment and pipeline of bulk plant. Domestic laws and regulations require that all the accounting data in the balance period should be the actual measurement value, while the holdup in equipment and pipeline can not be measured and can not meet the requirements of accounting evaluation. At present, the operator of nuclear facilities mainly adopt the empirical estimation method to estimate the holdup amount in process equipment and pipelines, with a large uncertainty. In the measurement of holdup, the international target value can not be achieved.

The target value realization relies on a variety of factors, combining with the actual situation in China, the topics of discussion are: the sub item uncertainty, holdup measurement, need of standard references, Carry out comparison activities , the establishment of certification bodies, including development of measurement software and so on. Careful planning and organization through certification bodies, enhancing the exchange of experience among various nuclear facilities will be a challenge in the future.

State
China

Gender
Male
Primary author: Mr LI, duohong
Presenter: Mr LI, duohong

Track Classification: PP: Nuclear material accounting and control

State Nuclear Security Technology Center (SNSTC) is the sole state-owned non-commercial service providing organization on nuclear security in China. SNSTC features in the comprehensive facilities on nuclear security and professional experts on nuclear security. Apart from the research and development in nuclear security, nuclear security training is also the mission of SNSTC. Since its beginning in November 2011, over 100 workshops have taken place in SNSTC covering nuclear material accounting and control, physical protection, detection of nuclear materials out of regulatory control and other relative topics.

In review of the training events from 2016 to 2018, we find out that scenario-based discussion is widely used in nuclear security training. For instance, the Regional Workshop on Counter Nuclear Smuggling on July 10-12, 2018 made use of the radioactive source theft scenario for discussion. We make the diagram to show the number of scenarios for training activities in the past three years.

In terms of themes, we analyze the characteristics of scenarios based on our practices. Scenario-based discussion increases interaction of training and combines learning with advanced tools. In a scenario which almost approaches real case, trainees actively think what they learn, use the learnt approaches to solve problems. Also, scenario can be shown in different ways by using some tools. It can be shown in printed materials, videos or other methods. Sometimes using virtual reality technology is also an efficient way.

It’s of great importance to develop credible scenario for nuclear security training. Based on our good practice in scenario development, we summarize the procedures for scenario development, which can be shared for efficient nuclear security training. There are three stages for scenario development, namely, pre-scenario development, scenario development in process, and post-scenario development. We take our practice of developing scenarios for case studies focusing on different themes of nuclear security training. For the case study of scenario development, the elements of the scenario, the steps to develop the theme-focused scenario are analyzed in details. In addition, the conclusion on the principles of scenario development is drawn.

Even for the same theme of training course conducted in SNSTC, we develop different scenarios due to the differences in the background of participants, the goal of training and other factors. In this case, the comparison to two scenarios focusing on the same topic is made. We want to highlight the flexibility as well as variety of scenario development.

The evaluation of scenario development is beneficial the sustainability of nuclear security training. The effectiveness of scenario development can be evaluated by trainees, participants and peers through interview, questionnaire and on-line survey. Some charts are shown for further analysis. The effective scenario development contributes to the success of nuclear security training. Our good practices in this regard will offers reference for our counterparts and promote the exchange of ideas among the organizations on nuclear security.

State

China

Gender
Female

**Primary author:** Ms SHI, Panpan

**Co-author:** Mr LIU, Xin

**Presenter:** Ms SHI, Panpan

**Track Classification:** CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for new-comer countries)
The development of LaBr3 detection system which can realize rapid identification and analysis of radionuclides

With the development of nuclear power, nuclear application and the challenge of nuclear terrorism threats, it is indispensable to monitor and control nuclear and other radioactive materials effectively in order to prevent proliferation and smuggling. Generally, radioactive materials can be identified by passively detecting and analyzing their characteristic gamma rays. Traditionally, energy spectrum analysis method, which statistically analyzes the gamma ray energy distribution based on Gaussian hypothesis, has been well developed and established and this method incorporating with HPGe (high-purity germanium detector) detector can identify radioactive material and precisely calculate its radioactivity. However, due to the long counting time resulted from the measurement of a large number of gamma ray events for low uncertainty of results, the energy spectrum analysis method is not suitable to be applied in security checking circumstance including customs, seaports, airports and checking points at borders. Typically, these radioactive materials waiting for inspection are put in shielded packages or cargo containers so that their characteristic gamma rays are easily attenuated and distorted.

This project studies the application of sequential Bayesian analysis method in the rapid identification of radionuclides. In this method, three “fingerprint” features of radionuclide, e.g. the decay half life, the gamma ray energy and the emission probability of characteristic gamma rays from different radionuclides, are jointly input into a model-based signal processor using the Bayes theorem and the sequential probability ratio tests theory, to make a judgment that whether the targeted radionuclides exists or not.

We developed a prototype of sequential Bayesian analysis system incorporating with a LaBr3 (Ce) scintillator detector to verify the feasibility of the sequential Bayesian analysis approach and to illustrate the detection performance (detection probability, mean detection time and false alarm probability) of this method varying as function of equivalent activity of the radionuclides. At the same time, the lower detection limit of the method is quantitatively evaluated.

State

China

Gender

Male

Primary author: Mr ZHOU, zhibo (State Nuclear Security Technology Center)

Presenter: Mr ZHOU, zhibo (State Nuclear Security Technology Center)

Track Classification: MORC: Detection technology development and performance testing
Nuclear Security – Integrated licence for Operation of first unit of Barakah NPP in the United Arab Emirates

This paper presents the process of the licence for operation of Unit 1 of Barakah Nuclear Power Plant (NPP) that has been followed by Federal Authority for Nuclear Regulation (FANR) in regards with the nuclear security requirements of the United Arab Emirates (UAE). FANR, the nuclear regulator of the UAE in accordance with the Federal Law by Decree No. 6 of 2009 on Peaceful Uses of Nuclear Energy, has to issue, for nuclear power plant, a construction licence and an operation licence (for loading of the fuel and operating the unit); the commission part is inside construction and operation licences. Through its Integrated Management System (IMS), FANR has established an integrated (safety, nuclear security and radiation protection) process for both licences of nuclear power plant. In the construction phase, the security team of FANR has mainly to focus on the protection against theft of category III of nuclear material when the nuclear unirradiated fuel is stored. FANR has to ensure that this storage of nuclear material is in accordance with the requirements of the regulation FANR-REG-08, for Physical Protection of Nuclear Material and Nuclear Facilities. For the operation of Unit 1 of Barakah NPP, the focus has to be moved to look more at the radiological sabotage issue. The process of licence for operating a Nuclear Power Plant has begun with the submission by ENEC (Emirates Nuclear Energy Corporation) to FANR of the Final Safety Analysis Report (FSAR). The FSAR followed the Preliminary Safety Analysis Report (PSAR), provided for the construction phase of the Unit 1 of Barakah NPP and includes a Chapter 20 on physical protection. The Chapter 20 is a summary of the Physical Protection Plan (PPP), which contains sensitive nuclear information not to be disclosed to the public. FANR security team has reviewed the PPP for operation as well as the associated documents such as the target sets analysis, the cyber security program manual, the vulnerability assessment and the contingency plan. During the period of reviewing, from 2015 to 2019, FANR security team has Request Additional Information (RAIs) – 150 - to ENEC and ENEC have answered in accordance with the regulation and/or the regulatory guides developed. The number of RAIs decreased to attain nil after the process is achieved. For the operation of the plant, it is also needed to verify that the plant has been constructed as per the requirements from the safety and the nuclear security. FANR has done this task through inspections. Especially, FANR security team verified that the physical protection system is conform to the description formulated in the PPP for operation. The findings were immediately communicate to ENEC to correct the observations before the loading of the fuel. Finally, FANR has to check the readiness of the unit to operate. FANR performed inspections and general exercises (emergency and security) to ensure that the unit is ready to operate. For example, FANR security team conducted inspection on the security organization on the site as well as all the related procedures. The security exercise has been performed by ENEC to demonstrate and improve the effectiveness of the Physical Protection Plan in the protection of the Nuclear Power Plant using scenarios up to and including the Design Basis Threat (DBT). For the issuance of the licence for operation of Unit 1 of Barakah NPP, FANR gathered the three following reports: the global Safety Evaluation Report (SER) on the FSAR, for both safety and nuclear security, the report on the findings of inspections (construction as design), the report on the findings following the inspection for readiness to operate and the results of exercises, for both safety and security.
State

United Arab Emirates

Gender

Female

**Primary authors:** Mrs ALSAADI, Sara (Federal Authority for Nuclear Regulation); Mr WINTER, Denis (Federal Authority for Nuclear Regulation)

**Co-authors:** Mr ALSHEHHI, Osama (Federal Authority for Nuclear Regulation); Mr AL HARBI, Mohamed (Federal Authority for Nuclear Regulation); Mrs AL MUHAIRI, Fatima (Federal Authority for Nuclear Regulation)

**Presenter:** Mrs ALSAADI, Sara (Federal Authority for Nuclear Regulation)

**Track Classification:** PP: Newcomers to nuclear power and research reactors: opportunities and challenges
How to react on signs of changes in behaviour that might be signs of concern?

In many countries there is some sort of screening in place as a preventive mitigation tool against the insider threat. A screening however, provides a picture of a person at a specific moment in time, based on the information that is gathered. Even though these screenings are conducted on a regular basis, it is still necessary to have some sort of follow up of those people who are working with sensitive material or sensitive information. A screening provides an overview of the past of someone, which we accept as an indication of behaviour in the future.

In Belgium, to have a concrete case, we have a security officer who will be responsible for demands of screenings and to follow up the people who are screened. It is however very difficult to have one person who is responsible for everyone in a facility. There should be a system in place where signs of changing of behaviour can be signalled in order to react.

In this setting it is important to define a baseline of behaviour. Without this baseline, you cannot define a change in behaviour. The difficulty is that every person is different and thus it is impossible to have a basic baseline and in cannot really be done by someone who is not in regular contact with the person him- or herself. It is therefore very important to identify the specific functions or people who are in the possibility to have this base of behaviour and can identify change.

During the international Symposium on Insider Threat Mitigation in March 2019 we have done an exercise on this topic. During this interactive session, we set out a specific profile and indicated a ‘baseline behaviour’. Based on indicated signs of changes in behaviour we challenged the group to think about when and how they would react.

During this exercise, with a sample of people working on insider threat, it was clear that it is a difficult balance on when to react. In general, one small difference in behaviour did not trigger any concrete reaction. Nevertheless when we put different small pieces of information together, most participants indicated they wanted to react. The different pieces of this new picture came from different parts of the facility: colleagues, HR service, line manager,... This is not information that is always brought together, which adds to the challenges of this subject. The reaction and the way it was conducted depends strongly on the legislative options and of the culture of the country, the company and the security culture.

In aftercare, it is a challenge to have concrete guidance, mainly because it depends so much on the legal possibilities and the culture. It is however clear that there needs to be some sort of system in order to follow up people who have been screened and that it needs to take into account different partners in the facility.

In this paper we would like to address these challenges and look and the different roles and responsibilities to report in an aftercare system.

State
Belgium

Gender
Primary authors: Ms DE LAET, Lisa (FANC); Ms CREUS, Christelle (FANC); Mr DRESSELERS, Rony (FANC); Mr SNOECK, Tony (FANC)

Presenter: Ms DE LAET, Lisa (FANC)

Track Classification: PP: Insider threats
Feedback experience from the IAEA missions with respect to Nuclear Security of Barakah NPP in the UAE

This paper presents the benefits to the development of the nuclear power programme in the United Arab Emirates (UAE), of the different missions performed by the International Atomic Energy Agency (IAEA) in regards to nuclear security for nuclear power plant. At the very beginning of the implementation of the nuclear power programme, the IAEA, on demand of the UAE, conducted an Integrated Nuclear Infrastructure Review (INIR) in January 2011. This INIR mission has a broader scope than nuclear security, to check the completion of the nuclear infrastructure for each of three phases (Phase 1: before the decision to launch a nuclear power programme is taken; Phase 2: before invite bids for the first nuclear power plant; Phase 3: before the commissioning and operating of the first nuclear power plant). The INIR mission was initiated for the first two phases and the UAE has prepared, before, a detailed self-evaluation report on the activities they have already done. Chapter 15 – security and physical protection – described the legislative and regulatory framework for nuclear security developed and to be developed, and the design basis threat (DBT) to be established as well as the protection of sensitive information. During this mission, the exchange between the IAEA team and the security team in both FANR, ENEC and CNIA was really fruitful for the development of the programme. The INIR 3 mission was conducted in July 2018 and, as a result, for the Chapter 15 – nuclear security –, IAEA proposed suggestions for ENEC and good practice for FANR to be detailed in the present paper. In March 2014 at the Nuclear Security Summit (The Hague, the Netherlands), the UAE stated in its progress report that an International Physical Protection Advisory Services (IPAS) mission will be provided to the UAE by the IAEA in 2016. The UAE requested by letter to the IAEA dated 3 February 2015 that the IAEA arrange an IPPAS mission in 2016 to assess the nuclear security programme of the UAE. From 29 October to 10 November 2016, the IAEA performed an IPPAS in the UAE. IPPAS is a peer review by IAEA expert on implementing relevant international instruments, in particular the CPPNM, its 2005 Amendment, and IAEA Nuclear Security Series publication, in order to assist member state in the establishment and maintenance of their national nuclear security regime. It was the first time at the AIEA that such mission is conducting during construction of unit. In this case, the scope of the mission was relatively narrowed to only focus on module 1 – national review of nuclear security regime for nuclear material and nuclear facilities; module 2 - nuclear facility review and module 4 - security of radioactive material and associate facilities and associated activities. The construction of Unit 1 & 2 of Barakah NPP was reviewed regarding these items. The UAE provided an Additional Information Package (AIP), which included relevant legal and regulatory documents, licensing and inspection procedures, facility specific information and a list of all documents relevant to nuclear security one month prior to the mission. The package was prepared involving all stakeholders in the nuclear security domain. The IAEA final report contained recommendations, suggestions and good practices, which will be used for the enhancement of the nuclear power programme in regards with the nuclear security. The IAEA, on demand of the UAE, has also performed other missions in the UAE such as Integrated Regulatory Review Service (IRRS), International SSAC Advisory Service (ISSAS), Emergency Preparedness Review (EPREV), which have little input in nuclear security. However, the IAEA advised and helped the UAE to build its nuclear security programme for nuclear power plant, by implementing the Integrated Nuclear Security Support Plan (INSSP) as well as the Integrated Master Work Plan (IWP) covering the nuclear sector. These plans provided national trainings and activities to be implemented in the security domain of the
nuclear power plant. From 2011 until this year, the UAE, with the help of the IAEA nuclear security division, has worked in nuclear security and finally achieved this task with the issuance of the licence of Unit 1 of Barakah Nuclear Power Plant.

**State**

United Arab Emirates

**Gender**

Male

**Primary author:** Mr AL SHEHHI, OSAMA (Federal Authority for Nuclear Regulation)

**Co-authors:** ALSAADI, SARA (FEDERAL AUTHORITY FOR NUCLEAR REGULATION); WINTER, DENIS (FEDERAL AUTHORITY FOR NUCLEAR REGULATIONS); Ms AL HAMMADI, FATIMA (Federal Authority for Nuclear Regulation)

**Presenter:** Mr AL SHEHHI, OSAMA (Federal Authority for Nuclear Regulation)

**Track Classification:** CC: Use of IAEA and other international guidelines for building national nuclear security regimes
The UAE’s regulation and licence for nuclear security transportation of Unirradiated fresh fuel

This paper presents the regulatory framework of the United Arab Emirates (UAE) for the nuclear security transportation of nuclear material and its implementation for the first licence of transportation of unirradiated nuclear fuel of Barakah Nuclear Power Plant (NPP). FANR, the nuclear regulator of the UAE in accordance with the Federal Law by Decree No. 6 of 2009 on Peaceful Uses of Nuclear Energy, has developed and maintained a regulation for Physical Protection of Nuclear Material and Nuclear Facilities [FANR-REG-08] to provide requirements to the operator of a nuclear facility. Based on IAEA recommendations of nuclear security series No. 13 (INF-CIRC/225/Revision 5), the regulation established requirements regarding the transport of Category I to III nuclear material (Article 27). FANR has developed a regulatory guide for Physical Protection for Transportation of Nuclear Material [FANR-RG-025] to provide guidance on how to respect the regulation. Before loading the fuel in Barakah NPP, the nuclear fuel has to be transported from South Korea to the UAE and stored inside the plant. The licensee of Barakah NPP, Emirates Nuclear Energy Corporation (ENEC), requested a licence for the transportation and the storage of fresh nuclear fuel in Unit 1 of Barakah NPP, in accordance with the regulations of FANR. In conformance with FANR-RG-25, the Transport Security Plan has been submitted to FANR. It was a recommendation in FANR-RG-25 to submit a Transport Security Plan to FANR, taking into account that the nuclear fresh fuel is Category III nuclear material, as well as to have an armed escort and Transport Security Centre. FANR reviewed this Transport Security Plan and Request Additional Information (RAIs) following the instruction for the Physical Protection for Transportation of Nuclear Material [FANR-SCD-RI-002]. In December 2016, the Licence for transportation of unirradiated fuel was issued and the Transport Security Plan was approved. From beginning of 2017 to August 2017, 5 shipment of nuclear material was organized between South Korea and Barakah NPP, fulfilling the approved Transport Security Plan. Before these transports, FANR has several meetings with the Nuclear Safety and Security Commission from South Korea as well as with Korea Institute of Nuclear Non-Proliferation and Control (KINAC) to discuss arrangements between the two parties in regards with the requirements for international transport of nuclear material in the Convention of Physical Protection of Nuclear Material (CPPNM) and its Amendment thereto. For the transport of unirradiated nuclear fuel of Unit 2 of Barakah Nuclear Power Plant and storage on the site, ENEC has to submit a Transport Security Plan to the approval by FANR.

State
United Arab Emirates

Gender
Female

Primary author: Ms AL HAMMADI, FATIMA (Federal Authority for Nuclear Regulation)
Co-authors: Mr AL SHEHHI, OSAMA (FANR); Mrs AL SAADI, SARA (FEDERAL AUTHORITY
FOR NUCLEAR REGULATION); WINTER, DENIS (FEDERAL AUTORITY FOR NUCLEAR REGULATIONS); Mrs AL MUHAIRI, FATIMA (Federal Authority for Nuclear Regulation)

Presenter: Ms AL HAMMADI, FATIMA (Federal Authority for Nuclear Regulation)

Track Classification: PP: Transport of nuclear and other radioactive material: practices, challenges and regulatory issues
FANR Cyber Security Regulatory Program at the UAE NPP

This paper presents first the regulatory framework of the United Arab Emirates (UAE) for Cyber Security at the nuclear power plant and secondly its implementation for the licence of Barakah Nuclear Power Plant (NPP). FANR, the nuclear regulator of the UAE in accordance with the Federal Law by Decree No. 6 of 2009 on Peaceful Uses of Nuclear Energy, has developed and maintained a regulation for Physical Protection of Nuclear Material and Nuclear Facilities [FANR-REG-08] to provide requirements to the licensee of a nuclear facility, including cyber security (Article 22). FANR established a regulatory guide for Cyber Security at Nuclear Facilities [FANR-RG-011] to provide guidance on the compliance of the regulation. This guidance was based on U.S. NRC Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities and IAEA Nuclear Security Series No. 17, Computer Security at Nuclear Facilities. In addition to the previous documents, the licensee could follow the Nuclear Energy Institute (NEI) 08-09, Cyber Security Plan for Nuclear Power Reactors. In the integrated (safety and nuclear security) licence process for operation of Unit 1 of Barakah NPP, Emirates Nuclear Energy Corporation (ENEC), submitted a Final Safety Analysis Report (FSAR), which contains a Chapter 20 on Physical Protection. This official unrestricted chapter referred to the Physical Protection Plan for Operation (PPP-O), which includes cyber-security. From 2015, ENEC developed the Cyber Security Program Manual (CSPM) and FANR reviewed it providing to ENEC more than 50 Request for Additional Information (RAIs). FANR wrote and finalized the Security Evaluation Report (SER) for the PPP-O, which has a part on cyber security. Moreover, ENEC established an implementation plan based on US NRC Cyber Security Milestones. FANR checked the implementation of the CSPM through inspections. The first inspection was conducted in Westinghouse office in USA in November 2016 to verify the system with protection implemented of cyber threat before its delivery at Barakah NPP. The second inspection was, on site, to verify the implemented part of cyber security (October 2017) and the third inspection was not completed because ENEC has delayed some worked to be done (March 2019). In final, to verify that the CSPM was correctly implemented as design, an inspection was performed in June 2019. All the findings were closed before the end of the 2019. FANR has reasonable assurance that the cyber security was implemented in Unit 1 of Barakah NPP as developed in the CSPM. As a result, the licence of operation of Unit 1 of Barakah NPP was issued in the beginning of 2020.

State

United Arab Emirates

Gender

Female

Primary author:  Mrs AL MUHAIRI, FATIMA (Federal Authority for Nuclear Regulation)

Co-authors: Mr AL SHEHHI, OSAMA (FANR); Mrs AL SAADI, SARA (FEDERAL AUTHORITY REGULATION)
FOR NUCLEAR REGULATION); WINTER, DENIS (FEDERAL AUTHORITY FOR NUCLEAR REGULATIONS); Ms AL HAMMADI, FATIMA (Federal Authority for Nuclear Regulation)

**Presenter:** Mrs AL MUHAIRI, FATIMA (Federal Authority for Nuclear Regulation)

**Track Classification:** CC: Information and computer security considerations for nuclear security
Experimental Testing and MCNP Modelling of Spectroscopic Radiation Portal Monitors to detect Illicit Trafficking of Nuclear Material

The threat of criminal or unauthorized acts involving nuclear and radioactive material has grown since the early 1990s. Each year IAEA reports loss, theft or out of regulatory control discovery of radioactive materials. Most incidents are minor, but material is potentially available for criminal acts. Illicit trafficking and theft of nuclear material can lead to nuclear proliferation and the possible construction of improvised nuclear devices or radiological dispersal and exposure devices. Measures to reduce the radiological and nuclear threat are many-faceted. An important component is the ability to detect illicit transport of radioactive and nuclear material. Fixed installed pedestrian Spectroscopic Radiation Portal Monitors are designed to be used at checkpoints such as those at road and rail border crossings, airports or maritime ports, to detect the presence of radiation in order to alert of the presence of nuclear or radioactive material. A combination of experimental data and simulations is a good way to study the performance of Spectroscopic Radiation Portal Monitors in realistic conditions. The paper presents a process to evaluate the performances of a portal, based on a combination of experimental data and MCNP simulations to calculate the detection probability and the false alarm rate for different measurement scenarios. IRSN developed platforms for testing Spectroscopic Radiation Portal Monitors for pedestrian control and collected experimental data from two Spectroscopic Radiation Portal Monitors, the first one is an available commercial radiation detection equipment and the second tested portal dates from the 80th but still present in nuclear facilities. Many scenarios were tested with different sources using realistic setups and many experimental data were collected using radioactive and nuclear material available in IRSN nuclear security laboratory. The tested equipment were simulated with MCNP based on the data provided in the user manual and the standards found in the industry. The MCNP model of the portal and its surroundings was adjusted to be as realistic as possible based on measurements performed with americium, cesium, cobalt, barium and europium sources. To get a realistic idea of the uncertainty, all the variables inherent in the measurement were considered. Their relative contributions were identified and quantified, then propagated to predict an overall uncertainty. The combination of experimental data, numerical simulations and uncertainty evaluation showed good agreement with experimental assays. The results were then used to test the sensitivity of Spectroscopic Radiation Portal Monitors to special nuclear materials for different alarm thresholds. This process applied to different scenarios according to defined targets should help in the selection of operating characteristics of the portal.

State
France

Gender
Male
Primary author: DEYGLUN, Clement (IRSN)

Presenter: DEYGLUN, Clement (IRSN)

Track Classification: MORC: Detection technology development and performance testing
Good Practices and Outcomes of the Asia Regional Network of Nuclear Security Training Support Centres

China, Japan and the Republic of Korea (ROK) drew statements that committed to establishing a capacity building support center in each country at the 1st nuclear security summit held in Washington DC in 2010. Based on the statement, each country respectively established a capacity building support center in December 2010 in Japan (ISCN: Integrated Support Center for Nuclear Nonproliferation and Nuclear Security), March 2014 in ROK (INSA: International Nuclear Nonproliferation and Security Academy), and March 2016 in China (SNSTC: State Nuclear Security Technology Center). Since the establishment, these centers have been actively in operation and providing training courses for national, regional and international audiences. Meanwhile IAEA, in the Nuclear Security Plan 2010-2013, commits to support States in developing Nuclear Security Training Support Centres (NSSCs) to facilitate human resource development and provide technical support at the national and regional levels. In order to support the member states with planned NSSC, IAEA held a preparatory meeting in February 2011 to launch the network and established “NSSC network” in February 2012. As China, ROK and Japan were working on establishment of similar NSSCs in the region, it was recognized among three parties to coordinate and cooperate, for example, by avoiding duplicate training courses among the three States. With this recognition, China, Japan, ROK established the Asia Regional Network (ARN) as a subnetwork within the NSSC Network in 2012. The ARN met in the margins of NSSC network annual meeting, facilitated by the IAEA, and initiated cooperative activities including information exchange and sharing of best practices. Since the establishment of SNSTC in China in 2016, SNSTC, INSA and ISCN have hosted “Asia Regional Network Meeting among China, Japan and ROK with IAEA (ARN+1 meeting)” every year in rotation since 2017. Through a series of ARN+1 meetings, SNSTC, INSA and ISCN have been strengthening the cooperative relationship in practical and meaningful ways including by exchanging information on training activities to understand each center’s strengths and coordinate schedules, sharing good practices and ongoing challenges to learn from each other, and sharing human resources by mutually dispatching instructors to the other centers’ training course. At the 3rd ARN+1 meeting held in May 2019, Japan, it was agreed by the 3 NSSCs and the IAEA to launch a joint project to jointly plan, prepare and organize technical visits to an operational NSSC in the region, to support developing NSSCs in neighbouring States on the area of human resource development in nuclear security. This paper describes the good practices and outcomes from the past activities of ARN+1 which is the first regional network of NSSCs in the world and foresees its future prospect.

State
Japan

Gender
Male
Primary authors: Mr NAOI, Yosuke (ISCN/JAEA); Ms LEE, Na Young (INSA/KINAC); Mr ZHEN-HUA, Xu (SNSTC/China); Ms SUH, In Young (Division of Nuclear Security, IAEA)

Presenter: Mr NAOI, Yosuke (ISCN/JAEA)

Track Classification: CC: Role of Nuclear Security Support Centers to support and sustain national nuclear security regimes
Design and Development of Mobile Based System for Doorway Monitor - TeleDM

Abstract
Radio Activity may spread in public places either intentionally or un-intentionally by any means out of any Nuclear Installation which may be catastrophic for the masses in general. There is a requirement of a system for detection and alarm annunciation of radioactive nuclides while there is any movement of Man/ Machine out of nuclear site. Also the alarm has to be communicated to concerned authority via SMS/MMS or any other communication means. Looking to the need of the hour, an indigenous, low cost, compact and portable, Mobile based Doorway Monitor system has been designed and developed. Mobile infrastructure is backbone for distant communication to be used by masses. Smart mobiles are compact devices yet powerful gadgets for designing new applications based on Mobile infrastructure. It has high processing power, good quality display, huge storage, user friendly interface with touch screen input and virtual key board. It has been used as a convenient way of interfacing to stand alone Instruments forming Compact Systems. Doorway monitor system is such a system and has been designed to monitor the presence of radioactive materials with persons who are coming out of Nuclear Power Plants, Radiation Labs and Radiological Installations. The system comprises of specifically designed doorway with a number of different detectors, the data of which is collected periodically by a Micro controller based Data acquisition Unit (MDU) via Blue-tooth connectivity. MDU will be responsible for sending the Count Rate information periodically to the local Smart Mobile based App. The application software running on the mobile phone (Android based) provides secure interface to the Doorway Monitor as well as saving of count rate data either on local storage or transmission of data to remote server/ cloud storage. Same data can also be displayed via ‘RemoteDesk’ application on any mobile connected with this local Mobile unit via internet. For different alarm annunciations, one Speaker with Amplifier may be attached to the local Smart Mobile unit. On detection of activity above set limit by the Mobile App, the system generates an alarm (vibration or sound, as per settings) in the mobile phone. The activities of various radio nuclides are displayed online on mobile Screen. Simultaneously, the mobile phone sends information about the activity detected and source identification automatically along with the location of the instrument (longitude and latitude), to a remote server and to multiple designated control room numbers. Based on this, necessary action can be initiated by the security personnel at central control room.

This paper details motivation for designing this system, new approach of designing Mobile based Doorway Monitoring System.

Key words: Doorway Monitor System, Data Acquisition unit, Bluetooth Communication

State
India

Gender
Female
Primary author:  Ms JAIN, VIDHI RAJESH (Head, R&D, La-Vastu Labh Pvt. Ltd., Vashi AND Visiting Faculty, CLE’S COLLEGE OF SCIENCE, ARTS AND COMMERCE, SECTOR 9A, VASHI, NAVI MUMBAI)

Co-author:  Ms JAIN, RANJAN BALA (Telecommunication Deptt, Vivekanand Education Society’s Institute of Technology, Chembur, MUMBAI)

Presenter:  Ms JAIN, VIDHI RAJESH (Head, R&D, La-Vastu Labh Pvt. Ltd., Vashi AND Visiting Faculty, CLE’S COLLEGE OF SCIENCE, ARTS AND COMMERCE, SECTOR 9A, VASHI, NAVI MUMBAI)

Track Classification:  PP: Physical protection systems: evaluation and assessment
Visualization and Machine Learning for Interactive Cyber Threats Analysis in Critical Infrastructures

Critical infrastructure is now under constant threat from cyber adversaries searching to exploit vulnerable systems and networks in order to achieve their targets (denial of service, sabotage, financial loss ...). As illustrated in the IAEA Nuclear Security Series No. 17 (Computer Security at Nuclear Facilities, fig. 7), the sophistication of attacks against computer networks is continuously growing disproportionately compared to the growth of defence technologies. Implementing computer security partly relies on strict levels of logging and monitoring of each entity of the system. As recalled in the IAEA reference manual, human errors and previously unknown threats have to be accounted for, to help investigators and operators take appropriate actions to mitigate risks. Therefore the supervision of nuclear industrial processes and related information systems is a mandatory component for security of nuclear facilities. The resulting logs and activity monitoring signals are gathered in a Security Operations Center (SOC). The role of SOCs is to supplement security tools (IDS, Antivirus, ...) by using machine learning, rule-based or manual investigation approaches to detect suspicious behaviours that deviate from usual and specified activities (anomalies). These additional detections usually generate a large number of alerts, which must be processed automatically or by an operator who is in charge of investigating the severity of these alerts.

This work proposes a software tool, combining machine learning approaches and visualization, designed to provide alerts with adequate supplementary information. The rationale is that a majority of alerts are generated because of a lack of synthetic and comparative knowledge of the involved entities or the generated events. A prominent example is the detection of some SSH-based communication protocols generated between a computer from the monitored network and an external computer. While this activity can appear as suspicious for non-specialized users, the history of the user enables a disambiguation of this kind of alert. Therefore, machine-learning approaches have been developed to model and summarize behaviours and to detect similar behaviours (computer, group of computers, external requests...). A key point of the tool is to offer investigators interactive 3D-based visualization, enabling simple and efficient data exploration with multi-level filtering and identification operations.

The visualization methodology relies on:

- Visualizing machine learning raw-data results: visualization helps security analysts to better understand what they are looking at and data-scientists what their machine learning algorithms do.
- Intuitive design for large-scale and heterogeneous data visualization.
- Efficient data exploration and multi-scaling alerts analysis.
- Adding interactive filtering and enabling graphical data selection.
- Interactive annotation and on-demand machine learning algorithms customization.
- Multi-view environment (from user-based activities to Domain-Name requests history summarization).

Various machine-learning algorithms are available in this tool, to enable efficient interactive exploration. Functionally, the goals of these algorithms are of three kinds:

1. **Behaviour modelling and summarization**: the aggregate history of a unique computer is usually difficult to interpret. Approaches have been developed to perform disaggregation
of activities into various classes, depending on the necessary level of implication by a human (e.g., periodic log activities have to be separated from other ones). Using pre-processed activities resulting from the disaggregation, events are then modelled through graph-based approaches. Such graphs are designed to naturally represent successive events linked together. The tool then offers graph-based algorithms developed in this context to summarize and characterize behaviours, which are occurrences of random walks on events graphs.

2. **Dimensionality reduction**: the analysis of various activities generate high dimensional spaces. A prominent example is the analysis of domain name requests by computers of the internal network. On an open network, the number of unique requests (number of requests for a unique domain name) can be of the order of a few millions, when observed over a few weeks. It is thus often desirable to perform dimensionality reduction on such spaces, to allow for subsequent manipulations within relatively small durations.

3. **Similarity search, top-k requests and clustering**: once users and events have been correctly described and summarized, it is crucial to allow the operator to perform various comparison actions. It can be of interest to perform a similarity search, which consists in finding entities, successive events, or a group of computers similar to an object already identified. This can be of upmost importance when specific behaviour resulting from a targeted attack has been identified and the investigator wants to ensure that no computer has been also attacked or infected. Variants of such a scenario include situations when the investigator wants to identify the k-most similar users to an identified one, or when he requests users or events to be clustered in a given number of groups.

The methodology and the tools are currently in test in operational configurations. Preliminary results show that it enables an efficient decrease in false positive alerts and helps investigators to better explore complex data and better understand relationships between multi-scale events using a 3D-based interactive visualization.

**State**  
France

**Gender**  
Male

**Primary authors:** AZZABI, Radhouene; MR GOUY-PAILLER, Cedric

**Co-authors:** MR VALLEY, François; MR DUBOIS, Hubert

**Presenter:** AZZABI, Radhouene

**Track Classification:** CC: Information and computer security considerations for nuclear security
Acceptance and Testing (A&T) Development in Malaysia Nuclear Security Instrumentation

Abstract: Nuclear instrumentation has served nuclear and radioactive detection and contribute substantial benefits to securities worldwide. Hence, the form and method to ensure that every equipment used is appropriate and comply with standards is essential for the ability of the detection of radiation. It also will increase public confidence of nuclear response teams facing nuclear threats. It is important to note that there are many types of instruments and models that are significantly different. As the technical agencies entrusted to overseeing nuclear security matters, Atomic Energy Licensing Board (AELB) began to explore an effective and sustainable means to develop indigenous capability in acquiring and maintaining detection instruments to ensure its operability and reliability. NSSC Malaysia through IAEA assistance, has been developed the nuclear security detection laboratory with the role to support and sustain nuclear security detection capability. As a genuine user country that depend on foreign technology for detection instruments, acceptance testing capability is critical to be mastered by country like Malaysia. Additionally, the standard of acceptance and testing (A&T) is an ideal and necessary upgrade to conventional technology in advancing nuclear security instrumentation. The recommendations cover the types of test to be performed, that has to be sought from various sources. This expertise is also extended to other frontline agencies such as Royal Malaysian Customs (RMC) and Royal Malaysian Police (RMP) in Malaysia in ensuring that the equipment owned by the relevant agency is capable of operating well and the national securities are fully protected. The knowledge is also shared regionally with interested countries.

State

Malaysia

Gender

Male

Primary author: Mr AB.RAHIM, Mohd. Hafizi

Co-authors: Mrs BAKRI, Noor Fitriah; Mr MOHD. TAHAR, Rozman; Mr MUHAMMAD JAMIL, Muhammad Zul Azri; Mr RADZUN, Hatman Riza; Mrs PUNGUT, Noraishah (Atomic Energy Licensing Board (AELB))

Presenter: Mr AB.RAHIM, Mohd. Hafizi

Track Classification: MORC: Detection technology development and performance testing
The Interface of Safety and Security in Transport of Radioactive Material

Once a country makes a knowledgeable decision to build a nuclear power plant, it must begin considering how to operate that facility safely and securely. It is important to continue working on the harmonization and integration of the safety and security areas in transport in order to develop a strong safety and security culture, taking into account the different historical evolution that both areas have experienced. It is intended to work on safety and security in an efficiently and effectively way, without duplication or conflict.

This paper assesses the prevailing safety and security culture and the degree to which it is successful in keeping people safe from radioactive materials. The paper also offers some guidance to small users that handle radioactive materials, regarding how they may enhance their own nuclear safety and security cultures. Joint inspections covering both safety and security issues have been performed. Sharing information, database, historical records, risks and threats are carried out in order to unify fulfilment for safety and security requirements.

The paper aims to describe the regulatory implementation of safety and security issues in the transport of radioactive material by the Nuclear and Radiological Regulatory Authority of Egypt – ENRRA– (Competent Authority for regulating transport of radioactive material in Egypt). It provides requirements in implementing and enhancing a nuclear security regime to protect radioactive material during transport. An effective legal framework is essential to ensure and facilitate safe and secure transport of Radioactive Material. Domestic legislation and international recommendations have an active role strengthening long-term control over the transport of Radioactive Material, and are periodically reviewed to ensure they remain effective. With the objective of controlling and monitoring the compliance with the applicable requirement of security standards, Regulatory Body must perform inspections and regulatory audits to consignors, carries and other related users.

The regulatory body in Egypt is in process of implementing a Data Base to store all information relevant to transport of radioactive material and the corresponding security measures: consignor, consignee, security, responsible, origin and destination of shipments, carrier, routes, type and amount of radionuclides (physical form, activity, etc.), models and approval certificates of packages, transport index, starting and ending date and time, quantity of vehicles and satellite tracking. The Data Base is used for recording the data related to Notice of Radioactive Transport forms submitted by users allowing, in this way, to have the orientative information about the quantity of land, air and water transports of these materials in Egypt. As Emerging technologies have a clear and significant role in enhancing the current security approaches, the paper is aimed to identify and apply modern technologies in promoting the security.

Security of radioactive material in transport continues to be a challenge for States that are working on strengthening their nuclear security regime. One reason for this is that State regulatory agencies and other organizations lack the resources and trained personnel to dedicate to this field. One way to assist States to advance nuclear security is to reach out to safety workers (regulators, inspectors, and safety compliance personnel) and showcase the need to better integrate safety and security practices.

Physical protection measures have become a matter of international interest and cooperation as well as a security plan during transport of radioactive material. Regulatory body of Egypt has the responsibility of requiring the Operator a complete Physical Protection system for radioactive facilities in accordance with the regulatory requirements set forth by it, as well as a Security Plan during transport of radioactive material. Regulatory Body carries out various activities related to the evaluation, monitoring and control of the design of the Physical Protection Systems and the implementation of practices.
Security Plans. The objectives of the requirements of physical protection of such materials during transport is assisted by minimizing both the total time the material remains in transport and the number and duration of transfers of the material, avoiding the use of regular movement schedules and limiting the advance knowledge of transport information including date of departure, route and destination to designated officials having a need to know that information.

**State**

Egypt

**Gender**

Male

**Primary authors:** Prof. EISAWY, Ezzat (Nuclear and Radiological Regulatory Authority); Dr FAHMY, Rania (Nuclear and Radiological Regulatory Authority); Dr KHATTAB, Abdalah (Nuclear and Radiological Regulatory Authority)

**Presenter:** Prof. EISAWY, Ezzat (Nuclear and Radiological Regulatory Authority)

**Track Classification:** PP: Transport of nuclear and other radioactive material: practices, challenges and regulatory issues
“Into touch with one another”: The sustainment of an Australian nuclear forensic capability through collaboration

“The history of science is rich in the example of the fruitfulness of bringing two sets of techniques, two sets of ideas, developed in separate contexts for the pursuit of new truth, into touch with one another”

J. Robert Oppenheimer

A robust and sustainable nuclear forensic capability will generally not, and did not in Australia, fall wholly within the ‘business as usual’ capabilities of a single organisation. Instead, it will draw upon the capabilities of multiple organisations, with dedicated efforts needing to be made to bring and keep these capabilities “into touch with one another”.

Organisations which form key parts of Australia’s nuclear forensic capability include ANSTO and the Australian Federal Police (AFP). These organisations typically function within entirely separate contexts; ANSTO is a public research organisation and the AFP undertakes operational law enforcement. These contextual differences in turn give rise to distinct characteristics in domains ranging from techniques and processes to organisational cultures. In spite of these differences, ANSTO and the AFP were able to come together to develop a national nuclear forensic capability. Over time it has become apparent that such differences are, in fact, critical to the success of this capability. For example, the traditional forensic techniques of fingerprint examination, DNA analysis and digital forensics have been brought together with glove box engineering developed over decades in the nuclear industry to establish capabilities for the examination of traditional forensic evidence contaminated with radionuclides. As a further example, processes such as chain of custody which are integral to the operation of a forensic laboratory have been integrated into the practices of the nuclear laboratory, ensuring that the results of the characterisation of nuclear or other radioactive materials will be accepted as evidence by the courts. The strengths of the Australian nuclear forensic capability has been demonstrated in activities such as the Nuclear Forensics International Technical Working Group (ITWG) Collaborative Materials Exercise 6 (CMX-6).

However, it is vital to maintain awareness of the challenges, as well as benefits, which can be presented by these contextual differences and implement measures to manage them as required. In Australia, such measures have included staff with tertiary qualifications in forensic science within ANSTO’s nuclear forensics team, programs of cross-training for staff of both organisations and formal agreements between the organisations which establish mutual expectations. However, organisations must not in this process lose sight of the key capabilities that they bring to the collaboration; the cultivation and maintenance of ANSTO’s unique nuclear knowledge and the associated technical proficiencies is fundamental to the national nuclear forensic capability.

This paper will describe the Australian model for nuclear forensics, built upon collaboration between ANSTO and the AFP, and provide examples of the ways in which the organisations’ capabilities are kept “into touch with one another”.

State
Australia

Gender
Female
**Primary authors:** KAITLYN, Toole (Australian Nuclear Science and Technology Organisation); BULL, Tegan (Australian Nuclear Science and Technology Organisation); KEEGAN, Elizabeth (Australian Nuclear Science and Technology Organisation (ANSTO)); GORALEWSKI, Jack (ANSTO); LEE, Samantha (ANSTO); LOI, Elaine (ANSTO); VAN DE VOORDE, Riley (ANSTO); YOUNG, Emma (ANSTO); RISTEVSKA, Slazana (Australian Federal Police); ROFFEY, Paul (Australian Federal Police); BURGER, Fiona (Australian Federal Police); CHO, Kaymann (Australian Federal Police); DAVIES, Beverley (Australian Federal Police); FRASER, Melanie (Australian Federal Police); GOODMAN-JONES, Andrew (Australian Federal Police); NELSON, Karina (Australian Federal Police); RENWICK, Stephan (Australian Federal Police); ROBERTSON, Geoffrey (Australian Federal Police); SCOTT, Daniel (Australian Federal Police); SHAW, Timothy (Australian Federal Police); STONE, Jennifer (Australian Federal Police); WONG, Andrew (Australian Federal Police); HOFFMANN, Emmy (ANSTO); APPERLEY, Miles (ANSTO)

**Presenter:** BULL, Tegan (Australian Nuclear Science and Technology Organisation)

**Track Classification:** MORC: Nuclear forensics
The current state of the nuclear security regime in Zimbabwe has drastically improved compared to the situation a decade ago. This is largely due to the introduction of legislation and a regulatory framework for nuclear and radiation sources. Since the commencement of regulation in 2009, a number of initiatives have been explored to strengthen nuclear security and the development and adoption of the Integrated Nuclear Security Support Plan (INSSP), which was adopted for implementation in 2013, accelerated the improvements being noted in nuclear security.

The development of the INSSP was instrumental in identifying all relevant competent authorities and creating an understating of their respective responsibilities in nuclear security. The level of nuclear security awareness outside the regulatory body was low and contributed to the weak regime that prevailed at the time. Further, the INSSP provided a platform for coordinating the various authorities leading to better cooperation. These included the regulatory body, customs, immigration, law enforcement, civil protection, environmental management, defence and civil protection among others.

This paper will explore the activities leading to the development of the inaugural INSSP for Zimbabwe adopted in 2013 and the key priorities that were identified as well as the benefits that were realized through implementation. Further it will highlight the key role played by the IAEA technical experts in the development of the plan as well as the implementation of individual planned activities, the main highlight being supporting nuclear security arrangements for the hosting of the World Tourism Organization (WTO) general conference in Zambia and Zimbabwe in August 2013.

Since the commencement of the implementation of the INSSP, a number of people from various competent authorities have been trained through national, regional and international courses. The training ranged from nuclear security appreciation to specialty training for frontline officers, nuclear security for major public events (MPE) and introduction to nuclear forensics. In addition, the country has been able to develop a nuclear security detection architecture strategy, development of concepts of operations (CONOPS), and a nuclear security response plan. The period also saw the procurement of mobile detection equipment some of which were wholly funded by Government through the regulatory body.

The changes in the nuclear security regime in Zimbabwe have made it less possible for nuclear and radioactive materials under regulatory control to be accessed and successfully used for illicit activities in the country or outside the borders. Similarly it has increased the chances to detect the movement of materials outside regulatory country especially at the main ports of entry and exit.

The paper will also highlight key success factors as well as challenges faced in the development and implementation of INSSPs and suggest how best these can be addressed for the benefit of countries embarking on the process or others facing similar challenges.

State

Zimbabwe
Gender

Male

Primary author: Mr CHIPURU, Justice (Radiation Protection Authority of Zimbabwe)

Presenter: Mr CHIPURU, Justice (Radiation Protection Authority of Zimbabwe)

Track Classification: CC: Identification of national needs through the development of an Integrated Nuclear Security Support Plan
Addressing IT security in nuclear security regulation and implementation with respect to interim storage facilities in Germany

There are currently 16 interim storage facilities for spent nuclear fuel in Germany in use. As IT-security is getting more and more relevant for nuclear installations, specific regulations regarding IT-security were integrated into the regulatory guideline for the storage of nuclear material. The responsibilities for interim storage facilities in terms of computer security in Germany, the BSI Act, which gives main regulations for critical infrastructure in the energy sector in Germany, the specific regulations for nuclear installations and their implementation are discussed in this contribution.

In 2013, a design base threat (DBT) especially for IT-security came into force in Germany. Based on this cyber-DBT, a completely new guideline for the protection of IT-systems, called "Guideline for the Protection of Computer Based Systems in Nuclear Facilities of Nuclear Category I and II against Malicious Acts", was created. This guideline includes IT-specific general objectives of nuclear security and addresses the computer security organization, the computer security concept and requirements for protection measures.

Essential measures resulting from the cyber-DBT, on the regulatory side as well as the practical realization in the licensing process are described. As a result, a process was initiated and is still ongoing in which IT-security is comprehensively addressed for all IT systems sensitive to IT-security.

Between 2013 and 2016 a plan with three milestones for the implementation of IT-security for all facilities of nuclear security category I, such as interim storage facilities for nuclear spent fuel, was designed. In 2014, the licence holder had to create a concept including an IT structure analysis. One year later a concept for the determination of computer security requirements and computer security zones had to be submitted. In 2016, the licence holder had to submit a complete computer security concept including the measures taken by the license holder. To specify the standards for the classification of the IT-systems by the operator, the Federal Ministry for the Environment, Nature Conservation and Nuclear Safety established additional exploratory notes.

As the starting point the IT structure analysis is a complete list of all sensitive computer systems of the interim storage facility including all interfaces and processes between these systems. During the second step of determining the computer security requirements, the computer systems were classified into four security levels (very high, high, increased and normal). Additionally, computer systems with the same security level could be summarized to computer security zones, to reduce the amount of separate systems for which special requirements have to be defined and fulfilled. In the final step the complete security concept should include the results of the former analysis as well as substantiated proposals by the operator for all measures taken against malicious acts.

The presentation concludes with a short outlook on future challenges in this field in Germany.

State
Germany

Gender
Female
Primary author:  WIESBAUM, Alice (Federal Office for the Safety of Nuclear Waste Management, Germany)

Presenter:  WIESBAUM, Alice (Federal Office for the Safety of Nuclear Waste Management, Germany)

Track Classification:  CC: Information and computer security considerations for nuclear security
Results of the 2019 IAEA workshop “Computer Security Approaches and Applications in Nuclear Security” in Berlin

Computer security within a nuclear security regime requires continuous improvement of computer security measures to face ever increasing adversary capabilities. For this one key factor is exchange of information (e.g. application of effective methods, technologies and tools in new and innovative ways) and identification of good practices nationally, regionally and globally. With this knowledge not only the national but also the international security level of nuclear material, nuclear facilities, other radioactive material and associated activities can be enhanced.

One possibility to exchange good practices and other interesting information in the field of nuclear security are meetings like the technical meeting “Computer Security Approaches and Applications in Nuclear Security” held in September 2019 in Germany. The objectives of this meeting are to discuss international, regional and national approaches to enhance computer security and describe implementations of computer security measures by organizations having roles and responsibilities within the nuclear security regime. Participants will be from different organizations and different roles such as executive management, regulatory bodies, computer security managers, administrators and technicians, physical protection system managers and administrators, sensitive information managers, and engineers from all domains of nuclear security.

In this presentation, an overview of the challenges and solutions of national and organizational approaches to computer security that can be used to protect sensitive digital assets specific to each domain of nuclear security (e.g. nuclear material and facilities, other radioactive material and associated activities, and material out of regulatory control) discussed at the 2019 IAEA workshop in Germany will be given. It also covers the ways computer security is applied in different countries. Further, current developments in international regulations on computer security are outlined. The approaches are compared, and differences are pointed out. Special attention is paid to experiences and best practices identified in different countries bringing the regulatory approaches into practice.

State
Germany

Gender
Female

Primary authors: Dr SOMMER, Dagmar; Mr BOSSY, Arnim; Mr NITSCHKE, Hartmut
Presenter: Dr SOMMER, Dagmar

Track Classification: CC: Information and computer security considerations for nuclear security
IAEA NUCLEAR FORENSICS TECHNICAL MEETING: BEYOND THE SCIENCE

Building upon the successful International Conference on Advances in Nuclear Forensics: Countering the Evolving Threat of Nuclear and Other Radioactive Material out of Regulatory Control (July 2014), IAEA convened a Technical Meeting on Nuclear Forensics in April 2019, Vienna, Austria. This meeting focused on the implementation of nuclear forensics in response to nuclear security events involving nuclear and other radioactive material out of regulatory control. With attention to human capacity building and the use of existing technical capabilities, the meeting featured shared experiences in the development and sustainability of nuclear forensics, as well as the conduct of a nuclear forensic examination. Over 150 participants from 80 Member States, INTERPOL and the European Commission attended the technical meeting and exchanged experiences involving the successful development of national nuclear forensic programmes and developed a vision for a stronger integration of nuclear forensic capabilities within national nuclear security regimes. Furthermore, the meeting reinforced that nuclear forensic science aims to reveal and establish links among people, places, events, and materials.

In keeping with the "Beyond the Science" theme, participants identified as an ongoing challenge the need to create stronger connections supporting the response to a nuclear security event, including the coupling of nuclear forensics science to the requirements of national legal systems as well as potential cooperation in investigations across borders. Many participants also stressed the need to foster and sustain the technical expertise and cross-disciplinary education of the next generation of nuclear forensic experts within both the scientific and law enforcement communities. Some highlighted the success of bilateral cooperation in applied training programmes and short-term nuclear forensics practitioner exchanges as ongoing efforts to tackle the concern of an aging workforce. Many countries showcased their experiences in establishing and sustaining national nuclear forensics capabilities, demonstrating how nuclear forensics has helped them to fulfill their nuclear security responsibilities and achieve a wide array of national security priorities, including enhanced border protection and stronger physical protection systems for their facilities.

In this presentation, the technical meeting co-chairs will present the "Beyond the Science" key themes and outcomes that will help advance the state-of-practice of nuclear forensics within the international community.

State

Other

Gender

Primary authors: Dr WALLENIUS, Maria (European Commission, Joint Research Centre); Dr WONG, Frank (US Department of Energy, Lawrence Livermore National Laboratory)

Presenters: Dr WALLENIUS, Maria (European Commission, Joint Research Centre); Dr WONG, Frank (US Department of Energy, Lawrence Livermore National Laboratory)
Track Classification: MORC: Nuclear forensics
A Revised Model for Nuclear Security Culture

The IAEA published the first model describing nuclear security culture in 2008. Based on that model, we developed quantitative and qualitative methods and collected data from eight nuclear sites in the U.S. The results from surveys, focus groups, and in-depth interviews were compiled and analyzed, shedding new light on the perceptions of nuclear security culture in these organizations. We compared the empirical data to the IAEA model to learn where there was convergence and divergence from the model. We identified some gaps in the model and characterized relationships between dimensions that were previously not well understood. Using this new knowledge, we created a revised model for nuclear security culture. The new theoretical model recognizes that security culture is developed within a larger environment that impacts overall organizational culture. Our data also suggest that management systems and leadership behaviors have the greatest impact on employee perceptions and security vigilance. It is the collective vigilance of employees within the organization that is the key determinant of security outcomes. We used the revised model to inform the development of a new nuclear security culture survey instrument. The validity and reliability of the instrument have been established. The instrument is being used to evaluate security culture at multiple nuclear sites in the U.S. The practical application of this research is that more meaningful measures of security culture are now possible. This tool can help organizational leaders understand how their workforce perceives security and provides insight into what perceptions can be influenced to have a positive impact on security outcomes.

State
United States

Gender
Male

Primary authors: Dr MILLER, Jeffrey (Oak Ridge Associated Universities); Dr SHAFFER, Matthew (Oak Ridge Associated Universities); Dr HAMMOND, Davyda (Oak Ridge Associated Universities)

Presenter: Dr MILLER, Jeffrey (Oak Ridge Associated Universities)

Track Classification: CC: Nuclear security culture in practice with a focus on sustainability
A comprehensive and integrated approach to the external protection of nuclear installations: the example of defense and security planning

The Specialized Command for Nuclear Security (CoSSeN), is an organisation created by the French Government in 2016. Supervised by the Interior and Energy ministries and composed of Gendarmerie and Police officers as well as civil servants, it aims to enhance the response of state security forces regarding physical protection of civilian nuclear facilities and transports.

As nuclear operators developed additional protection measures for their facilities, the state also reinforced the nuclear security regime by creating a new service.

The CoSSeN, along with other nuclear security actors, contributes to reinforcing the defense shield around nuclear facilities and transports.

It is the referent of the Interior ministry regarding actions of security forces to protect nuclear facilities and transports from malicious acts.

One of the main tasks of the CoSSeN is to enhance, harmonize and coordinate operational concepts.

In France, the "préfet", government delegate in the territories, is in charge of defense planning. This involves the following actions:

- They have to prepare the Nation, in all its components, state or not, to major crises;
- They have to ensure the continuity of the State and the essential functions of the Nation.

In this purpose, the CoSSeN is responsible for advising national and local authorities in the development of defense planning and national security.

Considering the great diversity of French nuclear installations, a specific site protection methodology has been elaborate around three axes:

A global approach:

- Coordination and involvement of all state stakeholders for the benefit of the authorities of the nuclear installation
- Risk and threat mapping
- State of the art of existing documents
- Safety engineering study for the four earth-air-sea-cyber dimensions
- Planning on all the functions of: vigilance, prevention, protection, and reaction

An integrated approach:

- Constant search for coherence between the exterior and the interior of the strategic site
- Consideration of the articulation between safety and security dimensions
Assistance dedicated to authorities and agents at the territorial level in their apprehension of the security problem of their site(s):

- Risks and threats awareness
- Implementation of requirements for the tools dedicated to project management
- Training
- Assistance in monitoring nuclear material transport
- Orientation of Intelligence Search
- Drafting plans
- Planning and organization of exercises
- Dedicated referrers as a consultant

**State**

France

**Gender**

**Primary authors:** Mrs DUBUIS, Mélanie (CoSSeN); Mr VILLEDIEU, Alexandre (CoSSeN)

**Presenters:** Mrs DUBUIS, Mélanie (CoSSeN); DEBIEVE, Chloé

**Track Classification:** PP: Application of the graded approach and defence in depth to nuclear security
Enhancing Global Cyber Security Capacity at Nuclear Facilities

Working with key nuclear industry cyber experts, NTI has developed the Cyber-Nuclear Security Forum to strengthen protection of civilian nuclear facilities from cyberattacks. A successful cyberattack on a nuclear facility could have serious consequences with global ramifications for human health and safety and the industry. The Forum seeks to support the cyber-nuclear experts working hard to defend their facilities against the expanding threat.

The Forum provides a venue for dialogue, information exchange, cooperation and problem solving among an international group of operational and technical experts addressing cyber threats at nuclear facilities. The Forum aims to: (a) enhance global cyber security practices and create an international network of experts by enabling engagement among experienced cybersecurity leaders at nuclear research and energy facilities; (b) accelerate and amplify the capabilities of the limited number of skilled, trained cyber-nuclear operators in nuclear facilities, particularly in countries without mature nuclear research or energy programs; and (c) establish an industry-led, self-sustaining vehicle that helps facilities get ahead and stay ahead of constantly evolving cyber-nuclear threats.

Nuclear energy and research facilities, including the sensitive digital systems used for nuclear security and safety, are not immune from cyberattack. Compromise of a facility’s business networks could lead to the loss of sensitive business information, as well as security-sensitive information that could enable future attacks, including sabotage. Compromise of digital control systems could directly affect the safety of a nuclear facility.

Given the global demand for such experts, all countries—but particularly countries with emerging nuclear programs that lack the hands-on knowledge gained through operating experience—are struggling to attract the technical talent needed. Even in countries with established nuclear programs, some utilities have a limited number of experts dedicated to cybersecurity. Given the intense competition for experts, inadequate technical capacity will be an enduring issue and one of the fundamental challenges for the global nuclear industry.

To address this issue, the NTI Cyber-Nuclear Security Forum seeks to promote greater international cooperation by engaging and building a network of cybersecurity experts from operational nuclear facilities. The Forum offers a necessary platform for global nuclear industry experts to cooperate and collectively strengthen defenses against cyber threats. This presentation will discuss the Forum concept and successes to date.

State
United States

Gender
Male

Primary authors:  Dr STOUTLAND, Page (NTI); DUMBACHER, Erin (NTI)

Presenter:  Dr STOUTLAND, Page (NTI)
Track Classification: CC: Information and computer security considerations for nuclear security
The Specialized Command for Nuclear Security and its role to control and monitor individuals access to the French nuclear facilities: The administrative investigations

The Specialized Command for Nuclear Security (CoSSeN), is an organisation created by the French Government in 2016. Supervised by the Interior and Energy ministries and composed of Gendarmerie and Police officers as well as civil servants, it aims to enhance the response of state security forces regarding physical protection of civilian nuclear facilities and transports. One of the main tasks of the CoSSeN is to control and monitor individuals accessing to nuclear facilities.

As a young institution in the nuclear security field, the CoSSeN helps to prevent and detect internal threats in the French nuclear civil sector, by centralizing, harmonising and coordinating the response of state security forces regarding the protection of civilian nuclear facilities and activities. For this end and to ensure an effective control of the individual access to nuclear facilities and protect our installations from any malicious acts, the CoSSeN has started to use ACCReD in 2017. This operating system allows, from nine Police and Gendarmerie databases, to check if an individual who requires an access to one of the civilian nuclear sites is known or unknown from the security forces and presents a risk because of his vulnerabilities. This system ensures a better control because all criminal records can be taken into account and it allows to give a relevant advice to the operator. It also allows the access to a dedicated program concerning those who have ties with Islamic radicalisation. For example, an access to a nuclear site can be refused to those who hold a criminal record for offenses such as consummation/dealing of drugs, violence, extortion, robberies or even those with the manslaughter charge.

In all the process, the CoSSeN only delivers a recommendation which allows the operator to make an informed decision and choose if the individual can or cannot access to the site. This decision can be contested by the person concerned to the Minister in charge of Energy within two months.

Thanks to ACCReD and the work of investigators and analysts, the CoSSeN has handled more than 536,000 investigations and approximately 5200 thumbs down. In a current year, the CoSSeN should carry out more than 400,000 investigations. This access control system applies to employees of major French nuclear groups (EDF, CEA, ORANO...), as well as numerous subcontracted workers. In addition to the knowledge and follow-up of nuclear workers, our organisation provides a better understanding of companies who are working with the major French nuclear groups. This operating system and more broadly the administrative investigation process are essentials to protect the internal security and public safety, and of course hard regulated by the law to not contradict individual liberties and rights.

State

France

Gender

Primary authors: Mrs DEBIEVE, Chloé (CoSSeN); Mr DELAROUSSE, Jean (CoSSeN)
Presenters: Mrs DEBIEVE, Chloé (CoSSeN); Mr DELAROUSSE, Jean (CoSSeN)

Track Classification: PP: Insider threats
The system of customs control of fissile and radioactive materials of the Federal customs service of Russia

1. General information.
2. Radiation control devices used by customs officers.
4. Prospect of development

State
Russian Federation

Gender
Male

Primary author: KOTOVSCHIKOV, Vladislav
Presenter: KOTOVSCHIKOV, Vladislav

Track Classification: CC: Nuclear safety and security interfaces
Establishing a sustainable regulatory framework for the security of radioactive sources through harmonization with a safety regulatory framework

For a State, one essential element of the security of radioactive sources is an effective national regulatory framework that provides for control over these radioactive sources. In many countries, the regulatory framework was initially developed based on safety concerns. Due to increasing concerns related to the security of radioactive sources and materials, States began to establish nuclear security regulatory infrastructures, either parallel to or in affiliation with the already existing safety regulatory infrastructures (e.g. using the same regulatory agency and/or competent authority for radiation safety).

In either case, there is a need to ensure that there is coordination and integration of safety and security frameworks in a sustainable manner. With respect to this, States must consider the consistency of regulatory functions, processes and requirements for both the safety and security of radioactive sources.

In order to establish and maintain sustainable nuclear security regulatory infrastructures for radioactive sources, it is important for States to understand the relationship between nuclear safety and security regulatory infrastructure requirements and recommendations. Some international requirements and/or recommendations in the area of safety and security of radioactive sources are identical or very similar, for example, the requirement for the establishment of a national registry of radioactive sources. However, some other requirements are unique solely to the security area, such as the requirement to examine the trustworthiness of employees, or solely to the safety area, such as the need to establish public exposure controls. Additionally, many requirements and/or recommendations fall somewhere in between, such as the need for effective authorization of facilities and activities, a regulatory inspection and enforcement regime and the graded approach to establish and apply regulatory requirements.

As such, the proposed paper will examine how international requirements and/or recommendations for establishing regulatory frameworks for safety and security relate to one another. The analysis will provide a detailed categorization of the range of requirements and/or recommendations in IAEA publications and will focus on identifying those that are essentially identical and those that are unique to safety or security. This will undoubtedly help States, experts worldwide, competent authorities and operating organizations to get a better perspective on the means and ways to harmonize, coordinate and integrate safety and security measures and systems into a strengthened sustainable regulatory framework for the safety and security of radioactive sources.
Primary authors: BACIU, Adriana (Brookhaven National Laboratory); Mr STERN, Warren (Brookhaven National Laboratory); Mrs ZIA, Sidra (Brookhaven National Laboratory)

Presenters: BACIU, Adriana (Brookhaven National Laboratory); Mr STERN, Warren (Brookhaven National Laboratory)

Track Classification: CC: National nuclear security regulations
Examining Gender Dimensions Amongst Nuclear Regulatory Authorities’ Leadership

The global community relies on national nuclear regulatory authorities around the world to effectively implement the world’s nuclear nonproliferation legal instruments and standards, including: The Non-Proliferation Treaty (NPT), International Atomic Energy Agency (IAEA) Safeguards Agreements and Additional Protocols, and the Convention on the Physical Protection of Nuclear Material (CPPNM). Evidently, national nuclear regulatory authorities play a critical role in implementing the international nuclear security legal infrastructure.

Meanwhile, women are frequently underrepresented in international forums on peace and security, including nuclear security. For instance, at the NPT Review Conference in 2015, 901 of the 1226 registered diplomats were men (73.5%) and 325 were women (26.5%). Closing this gap has been an important objective of the United Nations and the IAEA. In 2000, for example, the United Nations Security Council adopted Resolution 1325, which stresses the importance of ‘equal opportunities for the representation of women in all decision-making processes with regards to matters related to disarmament, non-proliferation, and arms control’. Similarly, IAEA Director General Yukiya Amano has stated that he would like to achieve gender parity at the most senior level of Agency staff by 2021.

Given the significance of the regulator’s role in the nonproliferation regime and recent research showing the benefit gained from embracing gender perspectives in peace and security, understanding the number of women in leadership positions in existing national nuclear regulatory institutions will help identify any gaps and areas for human resource development. This cross-cutting knowledge can help target efforts to increase women’s representation and effective participation at the national level and in the larger international nuclear nonproliferation regime, which can lead to improved nuclear security.

This paper will map gender diversity in the leadership among the national nuclear regulatory authorities as identified by the IAEA around the world. The study will begin by conducting literature reviews on the value of women’s representation and participation in peace and security discussions and decision-making processes and the typical role of a national nuclear regulatory authority as an implementer of the nuclear security regime. Next, the paper will share and analyze data collected by the author on the number of women acting as the person in charge of each national nuclear regulatory authority worldwide. This data will be collected by reviewing the websites of the regulatory authorities for information on gender diversity in their Mission Statements, Core Values, and Best Practices. The author will also conduct outreach via an email survey with a geographically diverse set of 10-15 regulatory authorities on their institutional approaches and practices to gender diversity.

In addition, this study will also present information on how nuclear regulatory authorities around the world approach and practice gender diversity within their institutions. In a similar fashion, this information will be gathered by reviewing the websites of the regulatory authorities for information on gender diversity in their Mission Statements, Core Values, and Best Practices. The author will also conduct outreach via an email survey with a geographically diverse set of 10-15 regulatory authorities on their institutional approaches and practices to gender diversity. In conclusion, this study will present 2-3 recommendations on ways in which national nuclear regulatory authorities can increase women’s representation and effective participation in implementing the international nuclear security legal infrastructure.

State
Gender

Female

**Primary author:** Ms VECELLIO, Mary

**Presenter:** Ms VECELLIO, Mary

**Track Classification:** CC: Nuclear security culture in practice with a focus on sustainability
Information technologies and digital transformation of customs control technologies for fissile and radioactive materials

1. The most important technological solutions for the digital transformation of customs control of fissile and radioactive materials;
2. The main organizational directions of digital transformation

State

Russian Federation

Gender

Male

Primary author: PESCHANSKIKH, Georgy
Presenter: PESCHANSKIKH, Georgy

Track Classification: CC: Information and computer security considerations for nuclear security
A Methodology for Monitoring Insider Threat

Insiders who may be staff members or contractors enjoy authorised access to a nuclear facility. Majority of insiders will be trustworthy. In spite of taking all the care in their recruitment, vested organisations may succeed in planting of mischievous elements or convincing or radicalising existing staff to implement their designs of terrorism. Use of insiders in creating trouble is obviously much more effective to them rather than attempting using terrorists from outside without insider help.

Insiders not only have authorised access to the facility but during their stay they acquire crucial knowledge which enables them to implement malicious acts with ease. An outsider will have to counter various levels of security apparatus which normally is very stringent in nuclear facilities. Outsiders may also need to try out number of trials in getting access to the sensitive material or information to perform act of terrorism to harm the facility and/or personnel. They may require more time also to do this and in process some alarm may get activated. If the response time by the security is short, they are likely to be nabbed or neutralised before they could perform their act. Insiders, thus are most potent means for terrorist organisations to implement their nefarious designs.

But before the insiders can perform their malicious acts, normally enough time is available with the organisations in which such elements can be apprehended. However, for security personnel to find out if something is cooking in their mind will not be an easy exercise. The best source to get such a feedback will from the fellow staff members who are in touch with the ‘insider’ on regular basis. They will be the first to smell any fishy designs. However, there is found to be considerable reluctance in reporting of such feedback by fellow staff members. Some of the reasons could be:

i) Have only suspicion but no evidence thus risking a colleague to become a foe
ii) May not have exact sense of the gravity of the issue
iii) Insider may be acting very friendly making them postponing or allowing the “insider” to mend ways
iv) May worry for their own or their family’s security to report against the “insider”

Because of the above, in most of the cases the required feedback may not reach the security authorities which in turn makes the best possible source of monitoring the “insider” ineffective. To obviate the above issues, a methodology is presented here to monitor “insider/s”. Any staff member’s activities will be in the radar of 8 to 10 other staff members in the facility or near his residence. Early signs of suspicious activities of the “insider” may get exposed to the immediate colleagues earlier than may be to his superior or security staff. The methodology consists in dividing the entire staff members of the facility into groups of say 5 or 6 persons. Any individual should be included in two different groups of staff members close to him thus making him common to two groups.

All staff members will be required to register their feedback which does not require naming anyone but requires only raising red flags about trouble in the group in which they are a member. A data acquisition system can be made to acquire and collate information received from a response pad provided to each staff member.

The response pad will have two sets of three buttons corresponding to the two groups he is part of. Green button will correspond to observance of no suspicious activity. Red button to indicate noticing terrorist related activity by a group member. Pink button may correspond to integrity issues. More such parameters can be added to make this exercise more comprehensive.

Red button may be selected for activities such as:

i) Meeting suspicious individuals
ii) Visiting radical websites
iii) Overhearing suspicious conversation
iv) Sudden change in behaviour
v) Early or late going from the facility without seemingly extra work assigned to him
Pink button will correspond to integrity related issues of a group member such as:
i) Sudden change in life style
ii) Becoming friendly with contractors, vising late night clubs etc.
All staff members in the facility should review and necessarily report on regular basis say weekly
by way of pressing Red, Pink or Green buttons as the case may be.
The collected data will provide information level of suspicious activities going on. Red or Pink
button in two groups in which one common member is there will indicate a particular individual
suspect. Available data will however, need to be analysed in more scientific manner.

State

India

Gender

Male

Primary author: Dr KOHLI, Anil (Consultant)
Presenter: Dr KOHLI, Anil (Consultant)

Track Classification: PP: Insider threats
Active Detection of SNM: Ten years of collaborative active interrogation work by the Atomic Weapons Establishment

Between 1993 and 2018 almost 3500 incidents of radiological/nuclear material being handled outside of regulatory control occurred, some 1250 were possibly related to trafficking and malicious use with 27 incidents involving Special Nuclear Material (SNM). Finding material outside of regulatory control presents many well understood challenges, not least of which is the potential for weak radiation signatures due to the standard constraints of time, distance and shielding. At issue is the potential to fail in the detection of such material which can, at face value, only be alleviated through the disruption of commerce by slowing cargo (increasing detection time), placing detectors right up against cargo (reducing distance) or opening cargo (bypassing shielding). An alternative approach is to increase the radiation signal by inducing fissions using an external source of radiation, thus allowing the resultant fission radiation signature to be detected through any shielding present on detectors placed outside the cargo, all within a timeframe which does not unduly interfere with the stream of commerce. This technique is termed Active Detection.

Since the turn of the century, Active Detection of shielded special nuclear material (SNM) for nuclear security applications has been the focus of a great deal of work by agencies worldwide. Inducing fissions in order to assay material is not a new concept and has been used since the 1960s for nuclear materials accountancy, processing/quality control etc. Such Active Non-Destructive Assay techniques tend to look to determine material mass/isotopics in geometries that allow small standoff in well characterised environments over long periods of time, the challenge is making this technique work in a border security scenario.

The Atomic Weapons Establishment (AWE) alongside the UK Government have maintained a programme to develop Active Detection techniques and technologies since 2008 and much work has been done, both by AWE and in collaboration with international partners during this decade. Significant progress has been achieved across a range of radiation sources, radiation detectors, data acquisition systems, and data analysis tools. This body of work leads us invariably to the conclusion that Active Detection works, that currently available technologies, when correctly configured and integrated, can successfully detect shielded SNM in a wide variety of realistic configurations. We describe ten years of experimental campaigns: from bench-top trials to multimillion-pound demonstrator systems, to show how the resulting data validates active interrogation as a technique, and discuss the remaining challenges.

**State**

United Kingdom

**Gender**

Male

**Primary author:** MARTIN, Philip (AWE)

**Presenter:** MARTIN, Philip (AWE)
Track Classification: MORC: Preventing illicit trafficking of nuclear and radioactive material
National benefits of strengthening nuclear security through tabletop exercises: perspectives from US communities

Summary:
A common operational strategy should unify and integrate Federal, State, and local response actions for the duration of a nuclear or radiological incident. However, coordination mechanisms and objectives of the different response groups will change depending on the phase of an incident. Incident response starts at the local community level with local first responders in the immediate aftermath of an incident. From the perspectives of U.S. local communities, this presentation demonstrates how tabletop exercises can strengthen nuclear security for enhanced cross-sector communications, cooperation, and integration among Federal, State, and local resources in the immediate aftermath of a nuclear/radiological incident. Moreover, national level tabletop exercises strengthen nuclear security by bringing together and strengthening the whole of government approach; promoting and cross-pollinating nuclear and radiological response technical experts; facilitating the development of local radiation-specific response plans; and raising awareness of current threats and the geographical and national resources available to counter them.

These perspectives, lessons learned, and observations are from the established Weapons of Mass Destruction (WMD) Counterterrorism Exercise Program within the Department of Energy, National Nuclear Security Administration, Office of Nuclear Incident Policy and Cooperation. Since its start in 1999, the WMD Counterterrorism Exercise Program has conducted more than 170 different WMD counterterrorism, preparedness, and response exercises across the United States and with key foreign partners, with over 13,000 international, Federal, State, and local participating officials. The program aims to promote awareness of terrorist threats associated with WMD materials; examine WMD counterterrorism prevention and response procedures, and exercise cross-sector communications, cooperation and team building.

Preparedness
• Strategy and the Planning Process: tabletop exercises bring together and strengthen the whole community to prevent, counter, and respond to a nuclear or radiological incident. Through the WMD counterterrorism tabletop exercise program, the Office of Nuclear Incident Policy and Cooperation has observed a number of local jurisdictions that have developed radiation-specific response plans, often including a communications component. These plans not only help identify and codify information pathways and roles for various authorities, but they also identify resources and available expertise both locally and provided by the Federal government. The plans also include the procedures for accessing those resources.
• Promoting Technical Experts: full community exercises (all levels of government) are not only a valuable tool for assessing plans, policies and procedures, but should be considered an opportunity to expose the response community to radiation subject matter experts.
• Cross-pollination of expertise: successful response to a nuclear/radiological incident relies on the acknowledgement of multiple expert communities, including: communications, radiation/health physics, and emergency response; by providing a forum for these communities to interact and learn from each other, they are better positioned to support public messaging during an emergency.
• Municipality planning case study from a U.S. city: operating in a regulatory environment necessitated by the proximity of two nuclear reactors has created an uncommon degree of familiarity with radiation and associated response plans. This experience enhanced their exercise performance and clearly impacts readiness.

Immediate Response
• Promote Awareness of Nuclear/Radiological Threats: tabletop exercises can raise awareness and subsequently enhance prevention and response tactics, techniques, and procedures, building an...
in-depth understanding of specific responsibilities which start at the local and community level.
• Exercise geographically specific resources: local authorities should be positioned to use networks and resources provided by specific sites, such as universities and hospitals. This facilitates a quicker response within a small community that may be directly impacted by a radiological event.
• Exercise phased actions and tiered response: coordinating structures start at the local level and are essential in aligning the key roles and responsibilities of Federal and State resources.
• Establish information pathways: while immediate messaging is ongoing, information pathways should be established to subsequently support more detailed and specific information as additional resources arrive. However, it is important to emphasize that immediate messaging cannot wait on the establishment of these information sharing pathways.

Long-Term
• By this time in the response/recovery, Federal assets will deployed to assist with long challenges
• The accuracy and consistency of early operations and messaging directly impacts the credibility of long term planning.
• Pathways for information sharing that support unified public messaging must be established early and these should be the same information sharing pathways that support response operations and response decision making.

State
United States

Gender
Male

Primary author: Mr ESTES, Derek (United States, Department of Energy, National Nuclear Security Administration)

Presenter: Mr ESTES, Derek (United States, Department of Energy, National Nuclear Security Administration)

Track Classification: CC: Good practices in the development and execution of nuclear security exercises (e.g. tabletop, drills and field exercises);
Nuclear Security Education and Training in Ghana.

Radiation sources and ionising radiation are widely used in various sectors of the Ghanaian economy which includes but not limited to Medical (General X-ray Units, CT Scanners, Dental, Fluoroscopy Units, Mammography, Radiotherapy and Nuclear Medicine), Industry (Moisture/density gauges, level gauges, thickness gauges, X-ray and gamma scanners), Agriculture, mineral mining, Oil and gas industry (well logging), road construction, breweries, NDT, other industrial facilities, Research and teaching etc. In addition, Ghana is one of the emerging countries embarking nuclear power project with projections to commence construction by 2023. In recent times, the security challenges associated with nuclear materials, facilities, and technologies are emerging at an alarming rate, necessitating corresponding counter measures. It is imperative therefore to establish education, training and tutoring which are key Components Needed to Develop and Maintain Technical Expertise for Effective Nuclear security regime. Ghana has invested significant resources in nuclear security education and training to meet the requirements of its future nuclear programme as well as existing facilities using Radiation sources and ionising radiation. The Department of Nuclear Safety and Security is one of the Departments of the School of Nuclear and Allied Science (SNAS) established in 2006 by the Ghana Atomic Energy Commission in collaboration with the University of Ghana. The Department offers MPhil and PhD Degree programmes in Health Physics and Radiation Protection and also an IAEA sponsored Postgraduate Education Course in Radiation Protection and Safety of Radiation Sources (PGEC). The mandate of the Department is to develop human capability and capacity in Radiation Protection, Nuclear Safety and Security. One main challenge in introduction of degree/ postgraduate programme in Nuclear security as in various developing countries is the national accreditation requirement of job prospects for graduates of nuclear security programme. Recognizing this challenge, Department therefore reviewed the programmes to introduce Nuclear Security as a core and elective courses into existing MPhil and PhD degree programmes in Health Physics and Radiation Protection Curricula. The department is determined to provide an appropriate national nuclear security human resource development programme which is essential in order to guarantee the sustainability of nuclear security knowledge and skills in Ghana. In this paper, the approach, gains and challenges of nuclear security education in Ghana is discussed.

State

Ghana

Gender

Male

Primary author: Dr KPEGLO, DAVID OKOH (Radiation Protection Institute/ Graduate School of Nuclear and Allied Science, University of Ghana-Atomic Campus)

Co-authors: Prof. FAANU, Augustine (Graduate School of Nuclear and Allied Science, University of Ghana-Atomic Campus); Dr LAWLUVI, Henry (Graduate School of Nuclear and Allied Science, University of Ghana-Atomic Campus)
University of Ghana-Atomic Campus); Prof. DAMPARE, Samuel Boakye (NATIONAL NUCLEAR RESEARCH INSTITUTE, GHANA ATOMIC ENERGY COMMISSION); Prof. SERFO-ARMARH, Yaw (Graduate School of Nuclear and Allied Science, University of Ghana-Atomic Campus)

**Presenter:** Dr KPEGLO, DAVID OKOH (Radiation Protection Institute/ Graduate School of Nuclear and Allied Science, University of Ghana-Atomic Campus)

**Track Classification:** CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
Cameroon’s Experience in Regulatory Oversight for Adoption and Implementation of Nuclear Security Regime

Radiation Protection Regulatory Bodies often have the responsibility of overseeing nuclear security activities, especially in developing countries like in the African Continent. Knowing that nuclear security, which is part of the national security system, combines the participation of several competent authorities, information management and the distribution of roles in general are stumbling points. The experience of Cameroon through the National Radiation Protection Agency (NRPA) is shared in this article.

NRPA took an active part in the expression of Cameroon’s commitment, in 2006, to implement the IAEA Code of conduct and it Guidance of import and export of radioactive sources. Similarly, NRPA was involved in the conduct of the process of ratification, in 2015, of the Amendment to the Convention on Physical Protection of Nuclear Materials and Associated facilities. Cameroon’s first Integrated Nuclear Security Support Plan (INSSP) that was implemented from 2013 to 2015 was oversighted by NRPA. NRPA also plays an important role in sensitizing stakeholders to the importance of nuclear security and their respective responsibilities. The source recovery or emergency exercises involving several competent authorities are often organized under NRPA’s leadership.

The limitation of access to, or confidentiality of some information is often not accepted by all administrative representatives. Those whose traditional duties are not linked to, hesitate to cooperate for nuclear security. Clear and precise regulation which sets out the roles and responsibilities of stakeholders is seen as the solution to this type of conflict for a harmonious coordination and arrangements of the national nuclear security regime.

State
Cameroon

Gender
Male

Primary author:  Mr SIMO, Augustin (National Radiation Protection Agency of Cameroon, P.O. Box 33732, Yaoundé, Cameroon)

Co-author:  Mr SAMBA, Richard Ndi (National Radiation Protection Agency)

Presenter:  Mr SIMO, Augustin (National Radiation Protection Agency of Cameroon, P.O. Box 33732, Yaoundé, Cameroon)

Track Classification:  CC: National nuclear security regulations
Nuclear security as part of the security of major public events: The African Heads of states Conference

I. THE CONTEXT OF THE EVENT: TERRORISM CONSIDERATION IN THE REGION.

II. PRELIMINARY ARRANGEMENTS OF THE EVENT

The political decision to undertake the major public event.


The inter-ministerial committees within the Agency including the general security committee for elaboration of the policy and strategies of the security of the event: its composition, organization and missions.

The competent authority responsible for the overall security of the event which is the Regional Security Council of Niamey: missions, organization and composition.

The general security plan of the major public event

The Nuclear security systems and measures into the overall security plan for the major public event: the institutions involved: the coordinating body, the development of a nuclear security system, the meeting, the trainings, the exercises, the equipment, the developed concept of operations and response procedures for appropriate detection and response measures, etc.

Organizational structure and coordination

Policy level;
Strategic level;
Operational level;
Tactical level.

III. PRE-EVENT ACTIVITIES

3.1. The nuclear and radiological threat assessment

This task consists of searching for and cross-checking all information related to theft, loss, abandonment, illegal trade or other illicit trafficking of nuclear, radioactive or other chemical or biological material at national or regional level.

3.2. Radiological research, monitoring and detection

Teams will conduct controls of nuclear and radiological substances perform the background noise mapping of radioactivity at the level of the following locations:
- The venue 1: Mahatma Gandhi International Conference Center (CICMG) and surroundings;
- The venue 2: Congress Palace and surroundings, etc.;
- Presidential and ministerial fairs of Diori Hamani International Airport;
- Hotels, Cities and Palaces intended to accommodate VIPs;
- Highways: the Airport-CICMG and CICMG-Hotels expressway;

The purpose of this prior check is to locate and detect any radioactive substances that could be the subject of a malicious act during the conference. It will also control the levels of abnormal ionizing radiation due to the presence of nuclear or radioactive material.

Teams are trained on the use of radiation detection devices. They will be provided with a backpack and an Identifinder and pager-type radiation detection devices.

The organization of the work: Each team will work for 72 hours in subgroups with a regime of 8 hours of work followed by a rest period of 16 hours.

IV. DURING THE EVENT
4.1. The access control and the patrol
Pedestrian and vehicular access control teams will be equipped with radiation detection equipment to detect and prevent all access to radioactive and nuclear materials. People on foot and/or on board vehicles will conduct patrols around the conference venue as part of the monitoring and detection of radioactive sources.

4.1. The Intervention of malicious acts involving nuclear or radioactive material.

4.1.1. Alarm evaluation team
Three teams of instrumental alarm control called “second level teams” will be installed for 48 hours not far from the various strategic locations (Airport, Conference Center and Palais de Congrès) to evaluate a timely alarm. Each team is composed of technicians and an investigator.

4.1.2. Emergency response team
A multi-service NRBC-E emergency response team will be installed near the conference venue for 48 hours to respond to malicious acts involving nuclear, radiological, biological, chemical or explosive material. It is made up of 28 people (investigators, Forensics experts, firefighters, environmental officers, EOD technicians, radiation protection officers, health workers and first-aid workers (see table below).

V. International Assistance and cooperation: The assistance of the IAEA

State
Niger

Gender
Male

Primary author: Mr RABIOU, Hambali (Niger National Police)

Co-author: Mr YAHAYA BAKO, Abdou salam

Presenters: Mr RABIOU, Hambali (Niger National Police); Mr YAHAYA BAKO, Abdou salam

Track Classification: MORC: Nuclear security in major urban areas
Good Practices for Creation of a Computer Security Regulation for the Nuclear Industry

The nuclear industry is changing. Industrial Control Systems and physical security systems are evolving from analog to digital equipment. There is a proliferation of microprocessors and operating systems throughout the system. Equipment that was traditionally connected via dedicated, hardwired connections and used proprietary protocols are now networked using more traditional Internet Protocols (IP). Although these systems were historically isolated, they are now being integrated with traditional information technology systems. We must now consider these systems from an integrated perspective. Threat actors are increasingly exploiting this integration to compromise key assets in other industries. These same tactics could be used to target and exploit similar systems at nuclear facilities.

The need for state regulation of computer security of the nuclear industry is clear. This will require computer security professionals to be part of a larger group to create and revise these regulations. Historically, they may not be familiar with the regulation development process and international good practices. This paper will provide a description of the beginning of this process.

The goal of regulation is to create an effective and efficient computer security program at sites which have nuclear material and radioactive sources. It is intended to provide clear requirements for the operators to follow. These requirements also provide clear expectations for the regulator to perform assessments at each site. The regulation will be used to create consistency between each operators’ computer security programs. The regulation also provides guidance and technical background where appropriate.

The IAEA’s NSS 17 (Computer Security at Nuclear Facilities) provides important guidance. Key sections of a computer security regulation will include, but are not limited to:

- The legal basis for the regulation
- Organization and management of computer security programs
- Roles and responsibilities for the regulator and operators
- Other involved organizations (law enforcement, national intelligence capabilities)
- Ensuring and prioritizing confidentiality, integrity and availability
- Design Basis Threat
- Account and user management
- Asset identification and characterization
- Identifying vulnerabilities and managing risk
- Provisions for the protection of Industrial Control Systems and Physical Protection Systems
- Understanding network topology and enforcing separation of communications by function and sensitivity
- Intrusion detection and prevention
- Incident response and recovery
- Training and awareness programs

The creation and revisions of computer security regulations is a critical process and must be carefully managed. The regulation must be properly organized to be easy to understand and implement by the operator. It must use normative language for clarity. They also must clearly define the role of the regulator and provide transparent expectations of their assessment of operators. Requirements must be clearly separated from recommendations, good practices, and background material. Requirements must also be clearly enumerated to facilitate communications between the operator and regulator. Only by being measurable can requirements be assessed. Regulators and operators
must form a partnership where impacts of policy can be openly discussed. Operators must be included early and often in the creation of these regulations. Each requirement carries a cost that will ultimately be paid by the consumer of the energy generated. The developers of the regulation must clearly understand the impact and burden on both the regulator and the operators. The operator must implement the requirements, and the regulator must assess the effectiveness of the implementation by the operators. This can cause significant and sudden impact and burden includes both manpower and costs. A plan to acquire additional funds will be needed and the lead time for that funding and the hiring of new personnel. One suggested approach is to pilot the implementation and assessment of a draft regulation with the regulator and a selected operator. This allows a more agile and quick regulation development process than the normal regulation enactment and revision process. This can be as simple as tabletop exercises, or full implementation of draft regulations. Another option is to utilize a phased approach to regulation enactment and requirements. Requirements can be added over time. Regulatory items that start as recommendations can become requirements over time. This allows operators to grow their computer security program in a phased effort over a longer time period. Before, during development and after development, there is a need for frequent and honest conversations between operators and regulators must continue. This will drive the successful implementation and revision processes.

State
United States

Gender
Male

Primary authors: Mr WHITE, Gregory (LLNL); Mr BROMBERGER, Seth (LLNL)
Presenter: Mr WHITE, Gregory (LLNL)

Track Classification: CC: Information and computer security considerations for nuclear security
Increasing Computer Security for Radiological Facilities

Increasingly, physical security systems are evolving from analog, hardwired equipment to digital, networked, Internet Protocol (IP)-based components which means that computer security must be considered when implementing physical security upgrades to protect radiation sources. The blending of physical protection systems with traditional information technology systems is advancing at such a rapid pace that the two can no longer be viewed independently or separately. Security systems are evolving from standalone hardwired devices to network-based devices where both power and data may be provided by a single Ethernet cable.

Radiological facilities have a challenge to stay abreast of the threat while accurately assessing computer security threats related to physical security systems protecting radioactive sources, mitigating the risks, and sustaining risk reduction. The primary computer security concern that face radiological facilities is an adversary who could use a cyber-attack to override a facility’s existing network controls and physical security measures, allowing them to facilitate a physical attack that could result in unauthorized and/or undetected access to radioactive sources.

The protection of radiological materials is covered in the IAEA’s NSS 11 (Security of Radioactive Sources) and NSS 17 (Computer Security at Nuclear Facilities) can provide users of radioactive sources with helpful information on computer security concepts and higher-level responsibilities, but it doesn’t give specific guidance on the specific computer security controls that a radiological facility should implement. It is also not sized appropriately for typical sites which have radiological sources. The ORS Cybersecurity Best Practices for Users of Radioactive Sources fills this void by recommending measures for developing a computer security program, implementing specific computer security controls appropriate for a radiological facility, and provides recommended measures to sustain the computer security program. To address these security concerns, ORS has developed a Cybersecurity Best Practices for Users of Radioactive Sources. The ORS best practices guide provides an overview of how physical protection systems have computer security issues and covers recommended best practices for sites to improve their computer security posture with a focus on computer security hygiene measures. The intended users of the best practices guide are regulators, site security officers, site management, and security vendors. Users of radioactive sources that are part of large organizations such as research institutes, universities, medical facilities, or large companies may have computer security programs. The best practices guide is geared towards users of radioactive sources with limited computer security experience to provide information for countering potential cyber threats to their radiological facilities.

We will discuss progress and capabilities of the ORS cybersecurity program. Training, awareness, and best practices are key to this program. So is enhancing the security configuration of installed equipment, and enhancing the environment that equipment installed into. We will discuss key accomplishments of the program and its impact on both domestic and international sites. Active collaborations with industry, regulators and international organizations will be described. Our future plans to implement continuing process improvement will be delineated.

State
United States
Gender

Male

Primary authors:  Mr BUTLER, Nicholas (U.S. Department of Energy/National Nuclear Security Administration); HERDES, Gregory (NNSA Office of Radiological Security); WHITE, Greg (Lawrence Livermore National Laboratory)

Presenter:  Mr BUTLER, Nicholas (U.S. Department of Energy/National Nuclear Security Administration)

Track Classification:  CC: Information and computer security considerations for nuclear security
Comprehensiveness of countermeasures against potential cyber and physical insiders at nuclear facilities

The countermeasures against potential physical insiders and especially cyber insiders is critically important at nuclear facilities (NF); this concern reflected in IAEA Nuclear Security Series documents: NSS-8 (NST-041), NSS-10 (NST-058), NST-47.

Insiders activities confirmed by accidents presented in internet. For example, oil dumping from turbine at Belgium NPP Doel-4 performed by insider (2015) or Stuxnet malicious software injection into uranium enrichment centrifugal system in Natanz, Iran (2009) that shows the necessity of security provision against insiders.

Insider have authorities, knowledge and access (including access to classified information) to nuclear materials and nuclear facility (NF) equipment and NF systems software: NPP Automatic Process Control Systems, Physical Protection Systems (PPS), nuclear materials accounting and control systems. It causes a necessity of special protective and preventive measures complex creation for risk reduction of insider appearance.

It is necessary to apply a complex approach for protection against potential insider (PI):

• in employment: trustworthiness testing multistage process.
• in the process of work: excluding of physical, legal, cyber and psychological ability to conduct a crime by staff prophylactic management, PI identification, detection of personnel close to discharging.
• during discharging/reduction procedure: discharging/reduced personnel authority decrease and information backup provision.

Special multistage trustworthiness assessment procedure shall be conducted for PI employment avoidance. This procedure includes interview, psychological testing, lie detector testing, social networks analysis, records on convictions analysis, tendency to drugs or alcohol addiction.

Also there is a necessity of rules failure analysis both physical (attempting to access into restricted area, attempting to carry out forbidden tools) and digital (attempting to passwords brute force, installing malware) including different types of security systems testing. Personnel behavior testing shall be performed inside and beyond of NF: expensive shopping, criminal contacts, hacking activities.

Besides trustworthiness testing it is necessary to perform general security procedures against insiders: staff access limitation (physical access into facility areas and informational access into information systems), identification of forbidden tools carrying out that could be used as insider’s tools (digital: laptops, mobile phones, 3-G modems; physical: cold arms, bench tools) etc.

Great attention should be payed to preventive measures against cyber-insider due to modern malware development; existing security software not always can protect against modern malware, especially against “zero-day” threat.

It should be mentioned that cyber-insider may be high-level qualified (in comparison with physical insider), for example, for security systems information acquisition or malicious software implementation.

In comparison of PPS and information security system effectiveness assessment methods it can be found that a time-line analysis method modeling of adversary penetration have implemented since 1980’s (in addition to deterministic approach). A modeling assessment method for effectiveness assessment in IT-area been applying since 2010’s (MITRE and CTF models). In 2015 a cyber-physical penetration of adversary been considering in common mathematical approach in
PARCAT software. Integration cyber and physical adversary in common approach also considered in SSPA “Eleron”.
All above mentioned measures including a large range of others, for example, psychological work with staff, multi-layers physical and informational protection and complex information security provision in NF automated systems provides sufficient protection level against physical and cyber insiders at Russian NF.
It is noteworthy that deterministic approach on security systems conditions assessment can’t assess level of protection fully correctly due to fast change of technologies (physical and especially digital) because of upgraded requirements of regulatory documents (and documents itself) been developed only in 2-4 years after new threats identification. Approach related to PI behavior modeling (in addition to deterministic approach in NSS-8) will be developed by SSPA “Eleron” under IAEA research project J02010 “Improvements in Preventive and Protective Measures against Insider Threats at Nuclear Facilities” (2019-2022) that could improve quality of PI identification in Russian and other IAEA member states NF.

State
Russian Federation

Gender
Male

Primary author: Mr ZHURIN, Sergey (FSUE ELERON - Rosatom)
Presenter: Mr ZHURIN, Sergey (FSUE ELERON - Rosatom)

Track Classification: CC: Information and computer security considerations for nuclear security
Strengthening the security on transport of nuclear and other radioactive material: challenges and actions for regulatory improvements in Brazil

This work describes actions carried out by CNEN (Brazilian National Nuclear Energy Commission, the national regulatory body) to improve Brazilian nuclear and radioactive material transport security regulations, in a context of a broad revision and updating process of the country’s regulatory framework regarding the subject. The new regulations aim to reflect the most recent international recommendations and guidelines, taking into account the peculiarities of each sector. Such revisions were deemed necessary due to changes in local and global threat scenario, the technology advances on detection/tracking systems and the fact that the local regulation in force (CNEN NE-2.01) hadn’t had major changes since 1981. CNEN NE-2.01 is applicable to the operational units whose activities relate to production, use, processing, handling, transport or storage of nuclear materials. It is being divided in three other documents, more specific and better targeted:

- CNEN-NN-2.01 “Security of Nuclear Material and Nuclear Facilities”;
- CNEN-NN-2.05 “Security of Nuclear and Radioactive Material in Transport”; and
- CNEN-NN-2.06 “Security of Radioactive Sources and Associated Facilities”.

In order to justify and accomplish such task, an extensive study of local and international documentation has been undertaken, which led to several conclusions that serve as basis on the elaboration of new regulations. Specifically for transport, CNEN-NN-2.05 was based on several IAEA Nuclear Security Series publications such as:

- NSS26-G “Security of Nuclear Material in Transport”,
- NSS-9 “Security in the Transport of Radioactive Material”,
- the Amendment to CPPNM and
- “Code of Conduct on the Safety and Security of Radioactive Sources”.

The most important conclusions and challenges identified during the elaboration of CNEN-NN-2.05 compose the results of this work, which include:

- Different levels of security (in terms of detection/tracking, delay and response) depending not only on the category of nuclear material, or radioactive sources in transport, but also on the practice involved;
- State-based evaluation of the threat, in more precise quantitative terms (design basis threat);
- Development/use of newer methodologies for vulnerability assessments (e.g. response times, alarm assessment times, simulation metrics and tools, tabletop exercises, force-on-force exercises, scenario analyses, neutralization data);
- Improving interaction and communication amidst different State and private stakeholders, such as intelligence agencies, consignors, carriers and consignees;
- Training and formation of stakeholders in order to maintain a well-established nuclear security culture;
- Multi-agency exercises to improve mutual interaction and capabilities.

From the results obtained from the study, it’s possible to conclude that the new local transport security regulation will reflect better international security good practices and provide more adequate requirements for design and evaluation of Physical Protection Systems on transport operations.
State
Brazil

Gender
Male

Primary authors: ALVES TAVARES, Renato Luiz (CNEN - Brazilian National Nuclear Energy Commission); ROZA DE LIMA, Alexandre (Brazilian Nuclear Energy Commission); Mr MONTEIRO FILHO, Joséli Silveira (CNEN - Brazilian National Nuclear Energy Commission)

Presenter: ALVES TAVARES, Renato Luiz (CNEN - Brazilian National Nuclear Energy Commission)

Track Classification: PP: Transport of nuclear and other radioactive material: practices, challenges and regulatory issues
Adult learning and nuclear security: the important role of adult learning educational practices for impactful cross-disciplinary nuclear security training

Adult learning and nuclear security: the important role of adult learning educational practices for impactful cross-disciplinary nuclear security training

Author: Mart Stewart-Smith
Affiliation: United States, Department of Energy, National Nuclear Security Administration
Email: Mart.Stewart-Smith@nnsa.doe.gov

Summary:
The human elements of nuclear security sustainability rely on the integration of the principles of adult learning into nuclear security training and exercises. Nuclear security is fundamentally cross-disciplinary with the intersecting roles of technical experts and researchers of multiple disciplines, non-technical security personnel, professional crisis communicators, and emergency responders. These communities need to be presented with training environments that expose them to essential nuclear security topics while allowing participants to learn from each other and contribute their experiences and unique situational problem sets to course instruction. Adult learning principles encourage trainers and facilitators to recognize the perspectives and traits of adult learners, draw on their diverse experiences, give learners a stake in the learning process, and provide the space for self-driven learning. Drawing from a variety of experiences in nuclear security training supported by the Department of Energy, National Nuclear Security Administration, Office of Nuclear Incident Policy and Cooperation (NIPC), this paper explores how adult learning principles can enhance both learning outcomes and the sustainability of nuclear security training.

Applying adult learning practices to nuclear security training and sustainability

"Principles of Adult Learning"

- Unique context of adult learning: In contrast to the traditional schools of thought for non-adult learning, the principles governing the effective education of adults are unique because they are informed by the traits that make adults different from young learners – namely experience. The particular learning context of adult education and training leans heavily on one’s experience, learning readiness, ownership of the learning process, future applications, and reason for learning. Understanding and accommodating the differing principles and practices of education for adult versus young learning audiences is an important step in crafting impactful nuclear security training.

- Experience: This paper considers two modes of integrating experience into the adult’s learning process: reflective practice and situated cognition. Designing training modules to draw upon the experiences of course participants encourages reflective practice and allows participants to situate new information in their own knowledge framework created by past professional experience and training. Engaging practical activities use situated cognition to create new experiences that help to contextualize training materials and add to their existing knowledge framework.

- Process: Adult learners will typically have the experience to be engaged participants in their own learning cycle with input and influence over motivation, orientation, involvement, activity, reflection, and adaptation. Taking advantage of the opportunity for a collaborative rather than prescriptive learning process is an important element of adult learning.

- Self-Driven Learning: adult learning is typically not considered subject-centered but problem-centered. In the case of nuclear security training, we find that participants are less likely to be specifically interested in learning, for example, about the fundamentals of radiation and radiation health effects, and more interested in the operational or clinical challenges unique to a radiological environment that an understanding of those fundamentals will allow them to address. Focusing
on the operational context and implications of radiation principles increases learner engagement, interest, and retention.

*Nuclear Security Applications*

Case Study: NIPC supports a variety of training and exercise programs that rely on adult learning principles to create productive learning environments for diverse groups of participants, both within the United States and for international partners. Examples and lessons learned from NIPC experiences will illustrate the impact the adult learning frame of reference can have on nuclear security training programs.

**State**

United States

**Gender**

Male

**Primary author:** STEWART-SMITH, Mart

**Presenter:** STEWART-SMITH, Mart

**Track Classification:** CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)

Venezuela is a country that does not have high power nuclear reactors, until now a cyclotron and a Cobalt-60 sterilization plant which is located in the Instituto Venezolano de Investigaciones Científicas (IVIC), both located in the Greater Caracas.

The only way to obtain radioactive materials for medical, industrial and research use is through acquisitions to foreign suppliers. Buyers must have the necessary legality to make acquisitions and clients must have the necessary tools and permits to manage and safeguard radioactive sources, in addition, radioactive waste management must be carried out to ensure protection of the environment and sources when they are no longer in use. However, these materials from the moment they enter the National territory must be informed to the corresponding National Authority (Office of Atomic Energy for the Industrial part and Sanitary Radiophysics for the Health sector) about their use, handling, detection and protection tools, as well as the control of radioactive waste and what to do in these materials.

For this reason, it is proposed to the National Authorities the design of a Database System for accounting and Control of Materials Outside of Regulatory Control MORC in Venezuela. The purpose of this system is to control radioactive materials: purchase, arrival of the source to customs, the journey made from customs to the place of management, its location and its disuse. In addition, it will have a registry of the companies, industries, hospitals and research centers that handle radioactive materials from both open and sealed sources, the storage states of the sources, the states of the detection devices (Detectors of area, cameras, alarms and emergency buttons), contact telephones of all persons belonging to these institutions, their functions, classification of management spaces and use of sources. Armor calculations, detection systems, security and waste status will also be taken into account.

The entire database will be completed between the Regulatory Authority and the final clients. Each source must include: calibration date, initial activity, lot number. Also, the MORC Control system must include Fire and police telephones to guarantee a timely response when presenting an emergency, theft or sabotage.

The database can be obtained through e-mail connections, sending a format where the Radiation Protection Officer must complete all the information required for the Regulatory Authority to check it through the scheduled visits.

All the data offered to the Regulatory Authorities will only be used for informative purposes to obtain a faster response and keep in mind that the unused sources are included in the accounting to avoid any type of loss, theft and loss. Maintain the alert status of these radioactive sources and make scheduled visits to ensure the safeguard until their final extraction. It also reports on the qualification of both the importing companies and the institutions that manage the sources, if they are registered or if they are updated, among other purposes.

This database system will only be managed by Nuclear Regulatory Authorities such as the Nuclear Energy and Sanitary Radiophysics Office and will be for Institutional use.

State

Venezuela
Gender

Male

Primary author:  Mr SABALZA, Walter (Hospital Universitario de Caracas)
Co-author:  Mr POSU, Alvaro (Hospital Universitario de Caracas)
Presenter:  Mr SABALZA, Walter (Hospital Universitario de Caracas)

Track Classification:  PP: National accounting and control measures of radioactive materials
Development of the Asherah Nuclear Power Plant Simulator for Cyber Security Assessment

Monday, 10 February 2020 12:15 (15 minutes)

This work presents the development of a nuclear power plant (NPP) simulator suitable for cyber security assessment. The NPP model is based on a pressurized water reactor (PWR) implemented using Matlab/Simulink. The Matlab/Simulink model, the Asherah NPP Simulator (ANS), simulates nuclear processes and controller’s system dynamics. ANS has been developed by the University of Sao Paulo, Brazil, under the International Atomic Energy Agency (IAEA) Coordinated Research Project (CRP) Enhancing Computer Security Incident Response at Nuclear Facilities (J02008).

The ANS core design is based on a 2,772 MWt PWR Babcock & Wilcox (B&W), which is well known by several studies published after the Three Mile Island (TMI) Unit 1 accident. The main NPP parameters may be found in the Nuclear Energy Agency/Organization for Economic Co-operation and Development (NEA/OECD) study. The use of the TMI core facilitates the use of the previous developed RELAP/PARCS core model for benchmark, verification and validation activities.

The ANS comprises the Nuclear Steam Supply System (NSSS): reactor core, pressurizer, reactor coolant pumps and u-tube steam generator (primary side); and the Balance of the Plant (BOP): u-tube steam generator (secondary side), turbine, generator, condenser, feed water system. The NSSS and BOP comprehends their subsystems’ controllers where needed. Control logics used in real NPP have been implemented within software or hardware controllers.

The ANS can run standalone, i.e. within a computer or a virtual machine, or in a hardware-in-the-loop (HIL) distributed architecture test bed. It is the heart of a comprehensive simulation environment, the ANS Test Bed (ATB), with advanced instrumentation and control (I&C) capabilities. The ATB allows digital operational technology (OT) and information and technology (IT) researching and cyber security assessment.

ANS features include network connection by means of the open communication protocol Modbus and of the open cross-platform machine-to-machine OPC Unified Architecture (OPC-UA) protocol. The research team developed two ANS interfaces that allows communication among plant processes and any hardware embedded controllers or processes. The PROC I/O INTERFACE and the CTRL DATA INTERFACE are Matlab/Simulink drivers that send and receive signals to assigned equipment within the ATB. These interfaces may be user configured so any of the simulated subsystems can be replaced by their real counterparts. Therefore, the ANS processes and controllers’ subsystems may be exchanged by programmatic logic controller (PLC), field programmable gate array (FPGA) or other real world physical equipment. Thus, specific sub systems, which perform dedicated safety or security functions within the plant, may be tested against cyber attack within the ATB. For example, the ANS integration capabilities include the exchange of the ANS pressurizer level controller by it is embedded real world physical counterpart within the ATB. Similar strategy can be applied to any controller or major process function.

Besides the ATB, a Configuration & Attack Terminal (CAT), integrated with the ANS, has been developing for attack initiation, data collection, data analysis and training purposes. The CAT preliminary cyber attack scenarios, implemented using the current ANS version, considered a model-based and hardware-based schemes. Besides I&C components, both preliminary schemes comprehend standard IT equipment. Exploratory results indicate that the ANS may be a valuable tool not only for digital research and cyber security assessment, but also for computer security measures development, training and information sharing.

REFERENCE


State

Brazil

Gender

Male

Primary author: Dr BUSQUIM E SILVA, Rodney Aparecido (University of Sao Paulo,

Co-authors: Dr SHIRVAN, Koroush (Massachusetts Institute of Technology); Prof. PIQUEIRA, José Roberto Castilho (University of Sao Paulo); Prof. MARQUES, Ricardo Paulino (University of Sao Paulo)

Presenter: Dr BUSQUIM E SILVA, Rodney Aparecido (University of Sao Paulo,

Session Classification: IAEA Coordinated Research Programmes for Information and Computer Security

Track Classification: CC: Information and computer security considerations for nuclear security
The Asherah Nuclear Power Plant Simulator (ANS) as a training tool at the Brazilian Guard Cyber Exercise

Brazil performed a singular cyber defence exercise in 2018 (from 3 to 6, July 2018): the first Cyber Guardian Exercise (EGC – Exercicio Guardiao Cibernetico). That exercise brought together 23 organizations, from the public and private sectors, in the first national drill towards increasing of performance and stability of cyber security of Brazilian critical infrastructure. The University of Sao Paulo (USP) participants of the International Atomic Energy Agency (IAEA) Coordinated Research Project (CRP) "Enhancing Computer Security Incident Response at Nuclear Facilities" (J02008) took part of that drill by planning the EGC nuclear cyber attackers’ scenarios. The second EGC will take place from 2-4 of July, 2019, in Brasilia, Brazil’s capital. Besides public and private organizations from the finance (Itau Private Bank, Caixa Economica, Central Bank of Brazil, Bank Santander etc); nuclear (Eletronuclear, Industrias Nucleares do Brasil, National Energy Commission (CNEN)); and defence sectors (Brazil’s Federal Police, Brazilian Army, Brazilian Navy and Brazilian Air Force); the electric sector (Eletrobras, Itaipu Binacional etc) will also be participating. It is expecting that the number of participating will increase to more than 40 organizations.

Under the IAEA CRP J02008, the USP research team has been developing a nuclear power plant (NPP) simulator suitable for digital research, cyber security assessment and computer security measures development. The NPP model is based on a pressurized water reactor (PWR) implemented using Matlab/Simulink. The Matlab/Simulink model, the Asherah NPP Simulator (ANS), simulates nuclear processes and controller’s system dynamics. The ANS is the heart of a comprehensive hardware in the loop (HIL) simulation environment, the ANS Test Bed (ATB). The ATB has advanced operational technology (OT) and information and technology (IT) capabilities. This simulator was designed based on a 2,772 MWt PWR Babcock & Wilcox (B&W). The ANS integration capabilities include network connection by means of the open communication protocol Modbus and of the open cross-platform machine-to-machine OPC Unified Architecture (OPC-UA) protocol. Two USP developed interfaces allow that simulated subsystems can be replaced by their real counterparts. ANS is the adequate tool for cyber security training.

The ANS has been developed to allow digital OT and IT research, to enhance cyber security response and prevention by capturing thermo hydraulics, neutronics and corporate knowledge on plant operation. By designing a first-of-a-kind NPP simulator that allows exchange of hardware and software and the capture of process and network data, we are extending the ability of engineers to incorporate their operational knowledge on cyber security. During the 2 EGC, the USP research team will be presenting the ANS capabilities as a research tool. In addition, two cyber attack scenarios exercises, hardware-based schemes, will be performed for the nuclear community to point it out the ANS training capabilities. Practical cyber security exercises are an effective procedure to teach the specifics of OT and IT security.

The ATB HIL scenarios includes four virtual machines (VM) running:
- ANS: Windows 7,
- IPFire firewall: Linux Appliance,
- Network Time Protocol server (NTP): CentOS Linux, and
- ScadaBR [6]: Windows 7.

Moreover, the reactor power controller and the pressurizer pressure controller will be running in a programmable logic controller (PLC) S7 1200. There are three subnets within the ATB training scenario.

One of the attack scenario considers a third party authorized worker connecting a laptop for maintenance, an engineering unauthorized workstation remote access, the exploitation of network vulnerabilities that lead to changes in the PLC behavior. The control of reactivity function is compromised and the facility impact is accessed after the attack. Both training schemes are set up to guide the students through all the necessary steps to understand the importance of training: objectives of the exercise, network topology, dynamic of the attack and lessons learned. The overall goal is
to go through the security wheel of secure, improve, monitor, test and improve. The exercise are set up to go from the technical point of view to realistic situations by including a logical flow of events. The realism of the exercise are based on the attacker’s goal towards a successful reactor power sabotage.

REFERENCES


State

Brazil

Gender

Male

Primary author: Dr BUSQUIM E SILVA, Rodney (University of Sao Paulo)

Co-authors: Mr CORREA, Diego Alves (University of Sao Paulo); Mr ANTUNES, Felipe Ramos (University of Sao Paulo); Prof. PIQUEIRA, José Roberto Castilho (University of Sao Paulo); Mr SOUZA, Francisco Carlos Salles de (University of Sao Paulo); Prof. MARQUES, Ricardo Paulino (University of Sao Paulo)

Presenter: Dr BUSQUIM E SILVA, Rodney (University of Sao Paulo)

Track Classification: CC: Information and computer security considerations for nuclear security
DEVELOPMENT OF A COMPREHENSIVE SECURITY PLAN FOR RADIOACTIVE WASTE DISPOSAL FACILITIES IN MALAYSIA

Any criminal or intentional unauthorized acts to critical infrastructures such as radioactive waste disposal facilities would undermine efforts to protect people, property, society and the environment either directly or indirectly through exposure to ionising radiation. With the aim of preventing a malicious act, security measures should be designed to deter malicious acts, detect and delay any unauthorized access or unauthorized removal of the radioactive material. A security plan document sets out the security measures that the facility implements to prevent the loss, sabotage, illegal use, illegal possession or illegal removal of sealed sources throughout their entire lifecycle, including while they are in storage or during transportation. The preparation of security plan document is adequately in line with the Nuclear Security Series Recommendation On Radioactive Material and Associated Facilities (NSS 14) to implement one of the basic security function which is a security management. Over the years the Malaysian Nuclear Agency (Nuclear Malaysia) has grown to become a leader for Research & Development on waste technology activities including radioactive waste management, processing and disposal, which includes sitting for a national repository. The Radioactive Waste Disposal Facility operates in accordance with the Atomic Energy Licensing Act (Act 304) 1984 and related subsidiary regulation, enforced by the Atomic Energy Licensing Board (AELB) as a national regulatory body. The development of a comprehensive security plan is one of the license conditions that Nuclear Malaysia needs to be complied with when decided to build a Borehole Disposal Facility as the ultimate solution to the increasing number of category 3 – 5 of Disused Spent Radioactive Sources (DSRS). The development of the document is based on the latest guideline document provided by the AELB, 'Security Plan Preparation Guide for Radioactive Material' (LEM/TEK 62 Sem.2). The preparation of this comprehensive document has proved to be a big challenge for Malaysia, that chose to be the first country to implement the disposal technology through the Borehole Disposal Facility, especially in describing best practises on security management that includes measures for both technical and administrative physical security, for facility not yet built. This document also completely described the overall nuclear security system to protect the radioactive material and related measure to threat level, response to any possible nuclear security event and the protection of sensitive information. This paper provides thoughts on how these challenges can be overcome and suggest improvements that can be made in the future to ensure the sustainability of nuclear security control in this facility is well established and guaranteed.

State

Malaysia

Gender

Male

Primary authors:  Mr RAMLI, MOHD KHAIRUL AZFAR;  Dr ABDUL RAHMAN, IRMAN;  Mrs
ZAINAL ABIDIN, NUR SHAZWANI;  Mr OTHMAN, MOHD SIDEK;  Ms HASSAN, HASFAZILAH

**Presenter:**  Mr RAMLI, MOHD KHAIRUL AZFAR

**Track Classification:**  PP: Nuclear security of new nuclear technologies (e.g., small modular reactors)
Implementing Cyber Security into an Existing National Nuclear Non-Proliferation Program – A Case Study

Cyber threat profiling and risk mitigation is critical to any nuclear state organization and should be considered as part of any comprehensive nuclear security program. Defining and evaluating the impact of the cyber threat to mission can be challenging. An existing national nuclear nonproliferation organization undertook an effort to incorporate cyber security activities into its program to address cyber risk. One of the primary goals of this endeavor was to develop a set of prioritized recommendations for organizational follow-through. The organization dedicated subject matter expert resources in the form of a cyber task force to support this goal. Opportunities were identified where cyber security could be built into each program including office level strategies and tools. Of course, no new identified threat vector is easily considered and incorporated into existing programs without impact. There are many obstacles to be overcome. Technically literate subject matter experts are difficult to find, management has comparatively less experience applying cyber security into their programs, and trying to change the culture to consider cyber security risk at policy and programmatic levels takes time and management attention. As an outcome of this process, a roadmap for program integration was developed including the establishment of a cyber support team. This paper will discuss the challenges and successes associated with establishing such a team.

State

United States

Gender

Male

Primary authors: Mr ANDERSON, Robert (Idaho National Laboratory); Mr HANLEY, Tim (US DOE NNSA); Mr VANDYKE, Shayne (Pacific Northwest National Laboratory); Mr HOFFMAN, Rob (Idaho National Laboratory); Mr GODWIN, Scott (Pacific Northwest National Laboratory)

Presenter: Mr ANDERSON, Robert (Idaho National Laboratory)

Track Classification: CC: Information and computer security considerations for nuclear security
Challenges in securing vulnerable radioactive sources in Senegal

BOYE Ndeye Arame Director General ARSN
TALL Moustapha Sadibou Director of inspections ARSN
Ababacar Sadikhe Ndao Director of Regulations and Authorization ARSN
Email: arame.boye@arsn.sn

SYNOPSIS
The security of radioactive material began to become a concern for the Regulatory Authority of Senegal, following the various discoveries of sources that were used and stored at sites during visits made as part of our inspection program. Radiation measurements at some medical, industrial and research facilities have uncovered radioactive sources such as Ra-226 needles, Cs137, Am241-Be and Sr-90 sources that have been formerly used and abandoned in places reserved for any type of equipment out of order or stored with very low safety measures and no security measures. The challenges of managing the security of these vulnerable and all-used sources have led Senegal, with assistance from the International Atomic Energy Agency, to develop its Integrated Nuclear Security Support Plan (INSSP) in 2014.

After these findings, the Regulatory Authority asked the managers of these sites to affix the necessary signaling and to put in place measures to prevent unauthorized access to, or removal of, the radioactive source. Steps were then taken to seek the support of the IAEA and other partners to find solutions either for repatriation to countries of origin or for strengthening nuclear safety and security.

The purpose of this article is to show how the Regulatory Authority has managed to first inventory a number of used and abandoned sources and then to characterize and condition them with the help of the IAEA to ensure their regulatory control and security. Support from other partners for inventory and training on nuclear security will also be shown.

References:
1. Law No. 2004-17 of 15 June 2004 on the Protection against Ionizing Radiation
2. Law No 2009-14 on nuclear Security and Radiation protection
3. Decree No. 2010-893 of 30 June 2010 on the organization and functioning of the Radiation Protection and Nuclear Safety
4. Law 2017-21 of 5 April 2017 authorizing the President of the Republic to ratify the Amendment to the CPPNM.
5. Law amending the law No 65-60 of 21 July 1965 on the Penal Code
6. Protocol with US NRC
7. National INSSP Plan

State
Senegal

Gender
Female

**Primary authors:** BOYE FAYE, NDEYE ARAME (AUTORITE DE RADIOPROTECTION ET DE SURETE NUCLEAIRE); TALL, Moustapha Sadibou (Autorite senegalaise de Radioprotection et de Surete nucleaire); NDAO, ABABACAR SADIKHE (Autorité sénégalaise de Radioprotection et de Sûreté Nucléaire)

**Presenters:** BOYE FAYE, NDEYE ARAME (AUTORITE DE RADIOPROTECTION ET DE SURETE NUCLEAIRE); TALL, Moustapha Sadibou (Autorite senegalaise de Radioprotection et de Surete nucleaire); NDAO, ABABACAR SADIKHE (Autorité sénégalaise de Radioprotection et de Sûreté Nucléaire)

**Track Classification:** CC: Implementation of national legislative and regulatory frameworks, and international instruments
Physical Protection Laboratory Roles and Function in Strengthening National Nuclear Security Strategy in Malaysia

Abstract: The Atomic Energy Licensing Board (AELB) seek to strengthen the capabilities and knowledge in nuclear security through the enhancement of roles and functions of our national Nuclear Security Support Centre (NSSC) with the support and cooperation from the International Atomic Energy Agency (IAEA). Through this effort and cooperation, a Physical Protection Laboratory for Radioactive Sources facilities was established at the AELB’s Headquarters (the “Laboratory”). The laboratory is expected to expand Malaysia’s NSSC capabilities in providing better and practical training on physical protection for authorized facility. The laboratory is equipped with nuclear security instruments to fulfil the objective of the physical protection system (PPS) in preventing sabotage and/or theft of nuclear materials and other radioactive materials at the facility. The installation at the laboratory will provide practical and hand-on guidance in order to accomplish nuclear security objectives either through deterrence or a combination of detection, delay and response mechanism. The laboratory is expected to compliment the Authorized User Training programmed offered under NSSC Malaysia and can be used to offer demonstrations of the operation, hands-on training, maintenance and practical exercises on working principles of physical protection equipment. Malaysian’s NSSC, through enhancement of this technical capabilities at the Laboratory intends to host national and/or regional training courses on physical protection introduction and security measures training for Regulators, Operators/licensees, Security Personnel and University academics involved in Physical Protection application and Studies.

Keywords: Physical Protection; Nuclear Security

State
Malaysia

Gender
Male

Primary author: Mr MUHAMMAD JAMIL, Muhammad Zul Azri (Atomic Energy Licensing Board (AELB))

Co-authors: BAKRI, Noor Fitriah (Atomic Energy Licensing Board (AELB)); Mr MOHD TAHAR, Rozman (Atomic Energy Licensing Board); Mr RADZUN, Hatman Riza (Atomic Energy Licensing Board (AELB)); AB. RAHIM, Mohd. Hafizi (Atomic Energy Licensing Board (AELB)); Mrs PUNGUT, Norraishah (Atomic Energy Licensing Board (AELB))

Presenter: Mr MUHAMMAD JAMIL, Muhammad Zul Azri (Atomic Energy Licensing Board (AELB))

Track Classification: CC: Role of Nuclear Security Support Centers to support and sustain national nuclear security regimes
Response Framework against Cyber-attacks and Computer Security Exercises conducted by NPP Operators in Japan

Olympic Games will be held in Tokyo in July 2020 and prior to the Olympic Games, several major international events would also be held in Japan. Against this background Government of Japan has been making big efforts to proceed with the preparation for the measures against cyber-attacks to computer based systems and networks that control critical infrastructure.

Regarding protection against cyber-attacks to nuclear facilities in Japan, the Nuclear Regulation Authority (NRA), which is the regulatory body of nuclear activities in Japan, rules regulations and inspects all the nuclear facility operators every year in order to confirm whether those operators establish and conduct protective actions for their computer based systems and networks along with the regulations. The NRA has strengthened the computer security of nuclear facilities through these efforts. In addition, it is also important to consider and develop effective response framework against cyber-attacks, and to confirm that the framework works without any problem. In this regard, this paper will present the outlines of typical response framework for nuclear facilities against cyber-attacks in Japan as well as the effectiveness of computer security exercises which nuclear facilities conduct in order to review the framework.

Concerning the response framework for nuclear facilities against cyber-attacks, the IAEA publication “Computer Security Incident Response Planning at Nuclear Facilities” proposes the concept of “Technical Authority (TA)”, which is an organization with specialized skills and resources for responding to computer security incidents. In Japan, the police organization plays the role of TA. When cyber-attacks happen at nuclear facilities, operators are responsible for securing safety of their facilities, and the police organization responds to the cyber-attacks with operators as TA. That is a characteristic point regarding the response framework in Japan.

Every Japanese local police headquarters has a cyber-crime inspection section and when nuclear facilities notify the police of being attacked by hackers, cyber-crime inspection officers immediately go to the facility with forensic devices and start inspection. In addition, the National Police Agency of Japan (NPA), which unifies local police headquarters, organized 13 cyber-attack special inspection teams and located the teams to 13 major cities in Japan in 2013. When a local police headquarters calls for cooperation to the cyber-attack special inspection team, the special inspection team is dispatched to the facility as soon as possible using helicopters if necessary.

With regard to computer security exercises, the guideline concerning nuclear facilities’ computer security, which was developed by the NRA in March 2018, recommends that operators should conduct computer security exercises regularly. It does not require to conduct complex and sophisticated exercises for the time being, although the NRA hopes operators to achieve such levels in the future. So the NRA accepts operators to conduct mere table top exercises that confirm procedures to notify the regulatory body, local police headquarters, local government, etc. of the on-site situation.

However, prior to the development of the guideline, some NPP operators proactively and voluntarily began to plan computer security exercises including the development of exercise scenarios, and conduct every year in consultation with the NRA and local police headquarters. Among those NPP operators, some have planned and conducted advanced computer security exercises, which are realistic and sophisticated enough based on the international situation surrounding computer security and emerging technologies. Cyber-crime inspection officers and cyber-attack special inspection team members also participated in those exercises as players. These efforts contribute
to ensuring close communication between operators and the police organization and improve response capacity against cyber-attacks.

In this paper, the outline of response framework against cyber-attacks in Japan as well as the effectiveness of a computer security exercise which certain Japanese NPP operator conducted in the past including outline of scenario and responses to incidents will be presented.

State
Japan

Gender
Male

Primary author: Mr TAKIKAWA, Takeshi
Presenter: Mr TAKIKAWA, Takeshi

Track Classification: CC: Information and computer security considerations for nuclear security
Needs-based Curriculum Development of Regional Training Program on Nuclear Forensics

As a regional Center of Excellence (COE) on nuclear security in Asia, Integrated Support Center for Nuclear Nonproliferation and Nuclear Security (ISCN) of Japan Atomic Energy Agency (JAEA) has been supporting countries in Asian region by providing training courses on nuclear security since 2011. ISCN applies Systematic Approach to Training (SAT) for its training activities, which consists of four phases: (1) analysis, (2) development, (3) implementation and (4) evaluation. For the phase 1, training needs analysis, ISCN has been using various methods including needs survey missions to Asian countries to interview the relevant ministries/organizations; open source research, information sharing with other COEs, and survey using questionnaire form. The paper will focus on the survey using questionnaire form to the target countries and discuss good practice of collaborating existing regional framework for cooperation to conduct such survey.

The Forum for Nuclear Cooperation in Asia (FNCA) consists of 12 member states in Asia, and there are various cooperative programs under the FNCA including Nuclear Security and Safeguards Project. One of the objectives of the Nuclear Security and Safeguards Project is to identify specific areas/topics which member states request assistance for capacity building, and nuclear forensics is among those identified topics. ISCN has been an active participant of Nuclear Security and Safeguards Project of FNCA, so that it decided to collaborate with the project to analyze detailed training needs for nuclear forensics using a survey format.

In order to develop a training course which fits the needs of trainees, the training needs analysis should be carefully and thoroughly conducted. ISCN developed a series of questions for FNCA member states to fill out regarding their current status of nuclear forensics capability, and tried to find the gap between ideal condition. For developing the questionnaires, ISCN referred to the IAEA Nuclear Security Series No. 2, "Nuclear Forensics Support" (NSS 2). NSS 2 identifies the national core capabilities to perform nuclear forensics activities, and based on those core capabilities, ISCN developed 10 themes for questions: (1) nuclear fuel cycle activities, (2) national framework and response plan, (3) incident response, (4) nuclear forensics laboratory, (5) nuclear forensics analysis, (6) nuclear forensics interpretation, (7) nuclear forensics findings, (8) international cooperation and assistance, (9) nuclear forensics capability buildings, and (10) needs for nuclear forensics cooperation in FNCA. Each theme contains multiple questions. All member states of the Nuclear Security and Safeguards Project answered the questionnaires.

After ISCN received the answers, it conducted detailed analysis of the results both quantitative and qualitative manner. The analysis showed that member states recognized critical role of nuclear forensics in enhancing regional/national nuclear security and had intention to develop capability of nuclear forensics. At the same time, the analysis identified gaps in (1) national framework, (2) nuclear forensics laboratory, and (3) nuclear forensics interpretation and findings.

With these analysis results, ISCN started to develop a curriculum for the regional training course on nuclear forensics, with support from Office of Atoms for Peace (OAP) of Thailand. The gaps ISCN identified contained both generic and more technical areas, ISCN decided to develop a series of courses, not just one course, with awareness-raising course and a technical course to follow-up the awareness course. In 2018, ISCN-OAP team developed a four-day training course for awareness raising consists of lecture, practical group exercise, scenario-based tabletop discussion, and facility tour. Lecture materials covered all the three gaps mentioned above, and group exercises complemented lecture to deepen the understanding by the participants. Most of the efforts were given to develop scenario for tabletop discussion. The scenario should contain all three gaps identified.
through questionnaire survey, and all the participants should be able to relate their job responsibilities to the scenario to join discussion. ISCN-OAP team came up with a scenario with three scenes and series of questions associated with each scene. ISCN hosted the regional training course on nuclear forensics in January 2019, and it received 16 participants from 12 countries. The paper will describe the methods ISCN has used to develop the questionnaire, and conduct analysis of the questionnaire results. It will also illustrate how ISCN-OAP team developed course curriculum, lecture materials, exercises and scenario for discussion in detail. Moreover, the paper will provide an example of nuclear forensics training program, and good practice of collaboration with the regional cooperative framework to conduct training needs analysis.

**State**
Japan

**Gender**
Female

**Primary author:** NORO, Naoko (Japan Atomic Energy Agency)

**Co-authors:** KIMURA, Yoshiki (Japan Atomic Energy Agency); OKUBO, Ayako (Japan Atomic Energy Agency); Ms CHANGKRUENG, Kalaya (Office of Atoms for Peace, Thailand); Dr OKUDA, Masahiro (Japan Atomic Energy agency)

**Presenter:** NORO, Naoko (Japan Atomic Energy Agency)

**Track Classification:** MORC: Nuclear forensics
Evaluation and Assessment of Nuclear Threat and Security Interfacing

A threat and security analysis concerning the Physical Protection System (PPS) of Nuclear material (NM) and Radioactive material (RM) is a complex sector because of their widely used in justifiable functions like in industry, medicine, agriculture and scientific research. But their probable factors may be misrepresented by the incorrect performer to achieve particular anti-state goal in the form of deterrence and violence. Besides, threats in the forms of terrorism are nowadays seen from terrorists obtaining NM and RM in order to expand and fabricate radiological weapons specially capitalizing by the spirit of the fundamentalism and extremism. Therefore, a threat and security analysis and evaluation relating to the PPS of NM and RM such as nuclear fuel, nuclear waste, other radioactive substances and associated facilities dependent on the number of disparate and non-quantifiable features. These features involve technical, organizational, political, ethical and national security issues, and must be approached on the basis of expert judgments and evaluations. Hence, this study presents a comparative evaluation and assessment of threat and security interfacing for structuring and investigating the total set of relationships contained in multi-dimensional and non-quantifiable problem complexes. It is especially useful for the initial structuring of very complex socio-technical issues when there is limited time and resources. A very good co-relation has been found between level of violence or deterrence created by the localized accumulation using fuzzy expert system (FES). The study also presents the evaluation of safety and security as well as the vulnerability with predictive analysis. Hence, relevant national and international community should treat equally the legitimate possession of the RM and NM from the viewpoint of terrorism impact. Additionally entry control and subsequent usages of management, legitimate organization must be incapacitated.

State
Bangladesh

Gender
Male

Primary author: Dr HOSSAIN, Md Altab (Department of Nuclear Science and Engineering, Military Institute of Science and Technology)

Co-authors: Dr AKBAR, Mohammad Shawkat (Bangladesh Atomic Energy Commission, Dhaka, Bangladesh); Mr MAWLA, Md Rosaidul (Department of Nuclear Science and Engineering, Military Institute of Science and Technology)

Presenter: Dr HOSSAIN, Md Altab (Department of Nuclear Science and Engineering, Military Institute of Science and Technology)

Track Classification: CC: Nuclear safety and security interfaces
Cyber Security Exercise For Nuclear Facilities in ROK

As of the publication of NSS-13 and NSS-17 in 2011, the member states of IAEA are giving more attention to nuclear security regime including computer security for nuclear facilities. Following the recommendation of IAEA, member states has applied various kinds of computer security plan for their nuclear facilities. However, the occurrence of computer security incident is inevitable as the threat mechanism evolves day by day. Moreover, modern type of nuclear reactor features digitalized instrumentation and control (I&C) systems, giving more attack-vector to cyber threats. Therefore, the necessity of cyber security exercise for nuclear facilities is kept increasing.

In case of Republic of Korea (ROK), the Act On Physical Protection And Radiological Emergency (APPRE) which aims to protect nuclear facilities from unauthorized removal of nuclear material and sabotage, was revised in 2015, requiring each nuclear licensees to establish and implement the computer security plan. Based on the act and related law, Korea Institute of Nuclear Nonproliferation and Control (KINAC) has prepared regulatory standard (KINAC/RS-015) in 2016 to assist and guide nuclear licensees to implement the computer security plan by following 7-steps; 1) CST composition, 2) CDA identification, 3) Defense in Depth and Incident Response, 4) Portable Media Control, 5) Integrity Controls, 6) Operational Controls, 7) Technical Controls. The implementation result of each step is evaluated by special inspection by KINAC.

In the meantime, following the revision of APPRE in 2014, nuclear licensees in ROK are required to conduct physical protection exercise. The cyber security exercise is considered as a part of physical protection exercise in its legal concept, but it is conducted independently from the physical protection exercise by nuclear licensees. Licensees in ROK had a grace period regarding the cyber security exercise in 2015. Since 2016, licensees shall plan and conduct cyber security exercise according to the act and KINAC evaluates licensee’s cyber security exercise.

As the special inspection of 3rd step finished in 2018, nuclear licensees in ROK are now prepared their own computer security incident response plan (CSIRP). Starting from this year, the cyber security exercise is practiced based on the CSIRP. This cyber security exercise in ROK, features threat scenario specialized for the closed network of nuclear facility and response scenario based on the facility-specific CSIRP.

To sum up, cyber security exercises for nuclear facilities in ROK has evolved since 2016. For the period of 2016~2018, as there was no specific reference for the conduct of cyber security exercise, KINAC and nuclear licensees closely collaborated on the determination of exercise goal, contents, development of scenario, and evaluation criteria. Since 2019, the CSIRP became a reference for licensees to test the readiness for the response of computer security incident. In this paper, we introduce the development of ROK’s cyber security exercise conduct and assessment methodology. Moreover, our domestic plan to improve the cyber security exercise framework is also going to be suggested.

State
Republic of Korea

Gender
Male
Primary author:  Mr RYU, Jinho (Korea Institute of Nuclear Nonproliferation and Control)

Presenter:  Mr RYU, Jinho (Korea Institute of Nuclear Nonproliferation and Control)

Track Classification:  CC: Information and computer security considerations for nuclear security
Assistance in the Development of the Nuclear Security Infrastructure in Newcomer Countries

The development of nuclear infrastructure in the States embarking on the nuclear power or nuclear research programme is associated with objective difficulties due to the limited national capabilities and competencies. Being responsible vendor of nuclear material and technologies for a number of new overseas nuclear facilities, including nuclear power plants and nuclear science and technology centers, we recognize importance of establishing sustainable national nuclear security regimes in the States. Assistance to States in establishing and maintaining of highly professional, qualified and experienced human resources is one of our priorities.

IAEA is a technical and professional organization that is playing a central role in coordination of international cooperation and providing technical support to its Member States, upon their requests, in building their national nuclear security regimes. In this regard, since 2017, Russian Federation has been providing on annual basis voluntary contributions, in kind and funding, for implementation of TC projects related to nuclear infrastructure establishment. These funds, according to the IAEA-Russian Federation agreement, are being used for training and development of human resources in States that are constructing or planning to construct NPPs.

We also assist our partners in building their national capacities through direct, bilateral cooperation. Our bilateral work in establishing of nuclear science and technology centers is an example of our direct assistance to the States. Frequently, such bilateral interactions are considered as more productive, since discussions of issues related to physical protection systems establishment often involve exchange with confidential information.

Within such direct interactions with a foreigner customer, the State Corporation for the Atomic Energy "Rosatom" and Rosatom Technical Academy provide organizational and methodological support in the development of all 19 elements of nuclear infrastructure in newcomer States, including in the field of nuclear security.

In the State embarking on the development of a nuclear security infrastructure, various state authorities and organizations with nuclear security functions are acting or are being created, between which clear coordination mechanisms should be established and their strategic and current tasks and work plans should be defined, taking into account the recommendations and approaches of the IAEA.

Based on our experience of cooperation with some countries, for example, Bolivia, Zambia, CIS countries and other countries, we have developed and offer a model of the nuclear infrastructure of a newcomer country, including in the field of nuclear security. The purpose of the model is to assist decision makers at the national level to plan and implement a national nuclear power programme or a national nuclear research programme, including the creation and development of an effective nuclear security regime, especially at the initial stage of its development. The model is a description of the target status of the State’s nuclear security regime, which should ensure the safe and secure creation and development of a national nuclear power programme in the country. In particular, the model presents approaches to the development of a legal and regulatory framework, the creation of technical and human resources with development over time.

In close cooperation with the State - recipient of Russian nuclear technologies, a roadmap is developed containing recommendations for the development of a national legal and regulatory framework, a set of nuclear security organizational and technical measures and systems; it also identifies the organizations responsible for their implementation and the timing for the implementation of the proposed measures and systems according to the IAEA Milestone Approach. Based on the
educational and training needs analysis of newcomer countries for the development of staff competencies of various government authorities and organizations with nuclear security functions, Rosatom Technical Academy developed and conducts a number of training courses on nuclear security issues that may be included in the roadmap activities, for example, on the design, operation and inspection of physical protection systems, physical protection of critical facilities, etc.

Key words: nuclear infrastructure, nuclear security, Milestone approach.

State

Russian Federation

Gender

Female

Primary authors: LABYNTSEVA, Marina (Rosatom Technical Academy); SMOLSKY, Alexander (Rosatom Technical Academy); ZUBKOV, Dmitry (Rosatom Technical Academy)

Presenter: LABYNTSEVA, Marina (Rosatom Technical Academy)

Track Classification: PP: Newcomers to nuclear power and research reactors: opportunities and challenges
Capacity Development of the Global Nuclear Safety and Security Institute in the Field of Nuclear Security

Capacity building for the development, implementation and sustainability of a national nuclear security regime and the physical protection of the nuclear material and nuclear facilities is a key objective and essential part of nuclear activities for States with an advanced nuclear power programmes and for those that are just starting to implement a nuclear power or nuclear research programme. This capacity includes, inter alia, training in the nuclear security and physical protection. In 1993, the Intersectoral Special Training Center was established to train Russian specialists in the field of physical protection, which was later transformed into the Global Nuclear Safety and Security Institute (GNSSI). In 2017, the Institute became part of the Rosatom Technical Academy.

In the first years of its existence, the Institute was, first, a national training center, carrying out practical training of specialists in the field of various aspects of physical protection. With active cooperation with various competent authorities of the Russian Federation and coordination with them of its activities in training specialists in the field of physical protection and security of critical state-owned facilities, the Institute has developed and regularly implements more than 60 training programmes, of which 20 are programmes in the field of physical protection of nuclear material and nuclear facilities. More than 8,000 Russian experts in the field of nuclear security have been trained at the Institute of from 1993 to the present.

Training programmes and training materials are based on a systematic approach to training, on the requirements of the Convention on the Physical Protection of Nuclear Material and its Amendment, the IAEA recommendations in the field of nuclear security, the Russian regulatory framework and the extensive experience of the State Corporation for the Atomic Energy “Rosatom” in the field. Initially focused on internal Russian customers, the institute accumulated the broadest practice and experience in area of establishing, sustaining and further development of human resource capacity for physical protection and security and is willing to share this knowledge with interested IAEA Member-States. Thus, the institute developed contacts with the IAEA, that is playing a central role in coordination of international cooperation and providing technical support to its Member States, upon their requests, in building their national nuclear security regimes, and other international organizations. In recent years special attention has been paid to the development of international cooperation.

In 2004, a joint project on cooperation in the field of nuclear security between the IAEA and the Russian Federation was launched. The goal of the project was to expand and adopt the scope, diversity and improve the quality of training in the field of physical protection, conducted at the Institute in Obninsk for international attendees - specialists from the IAEA Member States. Thus, the institute developed contacts with the IAEA, that is playing a central role in coordination of international cooperation and providing technical support to its Member States, upon their requests, in building their national nuclear security regimes, and other international organizations. In recent years special attention has been paid to the development of international cooperation.

In 2018 and 2019, together with the IAEA, an outdoor training ground modernization project was implemented. The material and technical base created so far includes 7 training laboratories, 3 computer classes, a modular pedestrian and vehicle checkpoints, 2 training grounds for engineering and technical means of physical protection, a test site for technical means of physical protection and other facilities.

It is important that the broadest range of detecting equipment appears at Obninsk test site and laboratories, while training is organized in a way to deliver principals of establishing and functioning of various systems and measures. These infrastructure and approach give opportunity without im-
posing requirements on any nuclear security, including physical protection, system. So, Member States specialists may independently define what fits the best their States and facilities’ needs. Each year, the Institute hosts several IAEA international and regional courses and seminars; in total, more than 1,100 participants from 54 countries were trained. These international and regional events are developed and aimed at broad range of audience: senior staff, practical specialists and even students. Many of these events foresee hands-on trainings on direct operation of various physical protection tools and means and are conducted at special training test site and laboratories.

Moreover, going beyond hosting and implementing various training events at its place, the Global Nuclear Safety and Security Institute is willing and ready to share its many years of experience in the capacity building in the field of nuclear security with other educational institutions and national competent authorities, including through active participation in the International Network of Nuclear Security Support Centers (NSSC) and the International Nuclear Security Education Network (INSEN); by creating an international school of instructors in the field of physical protection, and by the participation of representatives of the institute as experts and instructors in various IAEA activities for the human resource development and for the development of training material for the IAEA and national training courses.

Key words: capacity building for nuclear security, physical protection, human resource development.

State

Russian Federation

Gender

Female

Primary authors: SMOLSKY, Alexander (Rosatom Technical Academy); ZUBKOV, Dmitry (Rosatom Technical Academy); LABYNTSEVA, Marina (Rosatom Technical Academy)

Presenter: LABYNTSEVA, Marina (Rosatom Technical Academy)

Track Classification: CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
Development of Hardware-based Computer Security Controls for Advanced PWR Reactors

In advanced pressurized water reactors (PWR) as Korean APR-1400 and Russian VVER-1200, instrumentation and control (I&C) systems comprise of different data processing systems that utilize different network interconnections with different communication protocols. To provide data exchange between those several I&C systems, gateway devices play an important role in implementation of the I&C system of the plant in order to allow data transmission between different data systems based on different protocols. Currently, gateway devices, which are typically specific industrial computers, are incorporating software-based computer security functions to protect such data processing systems against potential cyber-attacks or intrusions which, if occurred, may disrupt the availability of such systems and/or integrity of data transmitted within the I&C systems and data networks. In 2016, IAEA introduced the application of field programmable gate arrays (FPGAs) in I&C systems of NPPs. FPGAs are hardware description language (HDL) programmable devices that have no processors or operating systems like that in computer-based (or software-based) systems such as programmable logic controllers (PLCs). FPGAs are being programmed by configuring its interconnections, which are typical digital logic circuits, so that the intended functions can be performed.

In this paper, hardware-based computer security controls, based on FPGA technology, are developed to perform computer security functions for protecting gateways devices. Although gateway devices are not safety-related systems, they provide, together with data diodes, a unidirectional data transmission from the safety side to the non-safety side of the plant main I&C system data networks. Such unidirectional data transmission should be maintained so that there is no data reversely transmitted back to the safety-related I&C systems. Plant parameters data is unidirectionally transmitted from the safety-related I&C systems to the gateway devices which collect and process such data and then forward it to the non-safety I&C systems. In addition, bi-directional data transmission and data acquisition existing between the gateway devices and non-safety I&C systems for the purpose of control and monitoring of the plant operation. Software-based computer security functions may be vulnerable to cyber-attacks or intrusions which, if occurred, may disrupt the availability of gateway devices causing failure of plant dynamic monitoring systems.

FPGA-based computer security controls have the advantage of being software-free devices so that an insider or cyber-attacker will be unable to compromise or bypass its functions to initiate a malicious act against gateway devices. Typical FPGA-based computer security controls will be placed between the redundant safety channel gateway devices and non-safety I&C systems such as information processing systems. Such FPGA-based computer security controls are intended to function as data packet filter and malware scanner. Such computer security controls will similarly perform like a next generation firewall (NGFW) technology which combines traditional firewall function with other Ethernet data network filtering functionalities such as deep packet inspection (DPI), intrusion detection system (IDS) or intrusion prevention system (IPS).

The methodology of development such FPGA-based computer security controls functionalities are based on a digital comparator X-NOR logic gate circuit function where an input data will be compared with reference data. Reference data inputs will vary depending on the intended function. For data packet filtering, if a match exists between input data and reference data, it means a data packet is authorized to pass. For malware scanner, if a match exists, it means that malicious data is detected which may initiate a connection block to protect a gateway device against failure and being unavailable.
The intended FPGA-based computer security controls functionalities will be verified using synthesis HDL simulation tools. Further work is planned to develop a prototype of such computer security controls using a specific Ethernet type FPGA kit and then test it in an Ethernet-connected computer network environment lab.

**Keywords:** PWR; I computer security; FPGA

**State**

Egypt

**Gender**

Male

**Primary author:** Mr IBRAHIM, Ahmed Salah Mahmoud (Nuclear Power Plants Authority)

**Presenter:** Mr IBRAHIM, Ahmed Salah Mahmoud (Nuclear Power Plants Authority)

**Track Classification:** CC: Information and computer security considerations for nuclear security
Regulator’s Roles for Sustainable Effort for Nuclear Security Culture in Japan

Fostering and sustaining a strong nuclear security culture serves as the basis for achieving effective nuclear security. While the effort for nuclear security culture should be implemented by each organization responsible for nuclear security, this effort may not be sufficient to continuously support nuclear security, if it is made merely based on organization’s initiative alone. A comprehensive national framework is deemed to be necessary to make this effort to be effective and sustained. In addition, with the consideration of an insubstantial nature of culture additional approaches as external stimulants are also necessary to facilitate organizations’ effort for nuclear security culture.

In addressing this need Japan takes an approach of a three-tiered national framework in order to ensure the practical and sustainable effort for nuclear security culture. This three-tiered framework consists of the State, Nuclear Regulation Authority (NRA) as a competent authority (CA) for nuclear activities in Japan, and licensees under the regulatory control of the NRA. The followings are brief descriptions how each tier operates. The State, at the top tier of this framework, has pronounced its political commitment to nuclear security culture, most noticeably in the form of the national statement at the two Nuclear Security Summits in 2014 and 2016. This political commitment provides the NRA, at the second tier, with an incentive to proactively foster a strong nuclear security culture in Japan. Accordingly, the NRA is empowered to have the authority to oversee the effort by licensees, at the third tier, for nuclear security culture. Specifically, the NRA requires licensees to develop and implement the plan to foster a strong nuclear security culture and demands the involvement of the top management, in a tangible way, in the implementation result of the plan. This plan and its implementation status, particularly the involvement of the top management, are to be examined by the NRA during a physical protection inspection of nuclear material. If the plan has not been properly implemented, the NRA has the authority to provide the licensee with guidance or instructions to take corrective action. In addition, the NRA regularly meets with licensees’ top management in person to communicate its expectation for their leadership in nuclear security, and if necessary, directly requests them to take the lead in fostering nuclear security culture. This NRA’s approach to licensees and to their top management, in particular, serves as a strong incentive for the top management to oversee the effort to develop and implement its own approaches, suitable for its situation, to foster a strong nuclear security culture. One such an example is to make nuclear security culture messages to be visible for security guards in order to heighten their sense of responsibility and professionalism for their daily duties. Another example is to notify the employees of matters that may not present immediate risks but suggest negative signs for possible degradation of the physical protection system as well as to share good practices that have been made for the improvement of the physical protection. In this way the variety of unique efforts for nuclear security culture are continuously sought and practiced.

Since the approach by the NRA to licensees could have a great influence on them, the NRA assumes important roles in fostering and enhancing nuclear security culture in Japan as a whole. Accordingly, the NRA is not only taking aforementioned various approaches for ensuring the sustainable effort by licensees but also is taking additional steps to facilitate their effort to be practical and effective, for example, by sharing its own practices within the NRA as a role model. In facilitating licensees’ effort the NRA understands that a careful consideration needs to be taken not to distort or misguide licensees’ effort due to its potentially great influence on licensees. It is particularly true with regard to the way to incorporate elements related to nuclear security culture into the NRA’s assessment of licensees’ physical protection system. In this regard, the NRA has accumulated the experience of repeating trial and error based on past experience to find a good balance to incorporate the cultural elements into its physical protection assessment.
With the understanding of its important roles the NRA is not only exerting regulatory oversight on licensees but also motivating them to advance their effort for nuclear security culture through, for example, role modeling. Based on these experiences this paper will present Japan’s nationwide approach with the focus on the regulator’s roles for ensuring practical and sustained effort for nuclear security culture.

**State**

Japan

**Gender**

Female

**Primary author:** Ms HAMADA, Kazuko (Nuclear Regulation Authority (NRA) of Japan)

**Presenter:** Ms HAMADA, Kazuko (Nuclear Regulation Authority (NRA) of Japan)

**Track Classification:** CC: Nuclear security culture in practice with a focus on sustainability
NUCLEAR SECURITY PROGRAM FOR THE REPATRIATION OF DISUSED TELEThERAPY HEADS IN PERU

ABSTRACT

Radioactive disused sources with high activity constitute a high risk for people and the environment if they are not managed in an adequate way until their final disposal. In Peru, are produced this type of disused sources due to their use in radiotherapy, into medical applications. There is a history of terrible accidents that have occurred in other countries due to this kind of sources were out of control. One of the best management options is the repatriation of those disused sources to other countries. The disposal of disused sources of Cobalt -60, with high activity and depleted uranium in their shield, require not only radiation protection but also nuclear security program where it is necessary to make previsions of a lot of money. The present work describes the repatriation of disused sources, with high activities, according an agreement signed by the Peruvian Institute of Nuclear Energy and the International Atomic Energy Agency. The IAEA provided the financial support for the implementation of a nuclear security and radiological protection program, where Peruvian and German professionals worked together in order to comply with the objectives of the Project. This also permitted the repatriation of disused teletherapy heads stored for more than 20 years in the centralized national storage. The operations considered the dismantling processes, preparation of packages type B, as well as the compliance with the peruvian regulations and the participation of the national policemen, as part of the nuclear security program during the the transportation of the disused sources.

Keywords: teletherapy heads, cobalt-60, disused sources, packahe type B.

State

Peru

Gender

Male

Primary author: Mr MALLAUPOMA, MARIO (INSTITUTO PERUANO DE ENERGIA NUCLEAR)

Co-authors: Mr CORAHUA, ANDRES (INSTITUTO PERUANO DE ENERGIA NUCLEAR); Mr GUIOP, LUDWIG (INSTITUTO PERUANO DE ENERGÍA NUCLEAR); Mr RAMOS, VICTOR (INSTITUTO PERUANO DE ENERGIA NUCLEAR)

Presenter: Mr MALLAUPOMA, MARIO (INSTITUTO PERUANO DE ENERGIA NUCLEAR)

Track Classification: PP: Transport of nuclear and other radioactive material: practices, challenges and regulatory issues
Developing a multi-year nuclear-cyber capability development training and education program

The cyber domain has evolved over the past thirty years from one that was primarily concerned with the protection of data confidentiality, integrity, and availability, to one that includes an integrated set of defensive technologies and processes in order to respond to the ever-advancing threats posed by skilled cyber actors. As the cyber threat actors have evolved their capabilities, it has required that defenders not only deploy defensive cyber capabilities and skilled cyber defense staff to handle these tools and data, but also extend their training and education programs to include all staff such that the entire organization is considered as part of the cyber defense team, identifying and reporting observations that may indicate that a cyber-attack has or is taking place.

The nuclear domain for this same thirty years has included programs to address the protection and nonproliferation of nuclear materials through programs for physical security protection, insider threat mitigation, nuclear material accounting and control, transportation security, protection from sabotage, and incident response. It is only in the past ten years that cyber-security has become a capability of concern, not only as applied to these existing security domains, but also by itself as the attack surface within a nuclear facility is large and includes interaction with a diverse multifunctional staff. To address these security concerns countries such as China and the United States have established nuclear security centers of excellence in support of developing capabilities that contribute to mitigating the overall risk of handling and using nuclear materials.

Over the past three years the US and China have been working together at the State Nuclear Security Technology Center (SNSTC) in Beijing, China to implement a multi-year nuclear-cyber capability development training and education program. This program was built using US NIST Special Publication 800-50 on building an Information Technology Security Awareness and Training Program that includes a basic curriculum allowing students to progress from awareness programs to training courses to specialized domain education, with all course materials derived from existing risk and threat assessments. These courses are being implemented at the Center of Excellence in Beijing that is a multi-building site modeled with common nuclear facility capabilities including physical security zones and associated protection technologies, a functional Central and Secondary Alarm Stations (CAS/SAS), a material processing facility, and a material storage vault. This infrastructure allows for all courses from awareness through advanced to be offered with a hands-on component.

This paper presents the co-developed capability development training program including a history of the courses conducted that informed the creation of the structural levels and how this information was mapped to China’s existing operational training programs for completeness. Program course levels include awareness, basic training, intermediate-to-advanced training on specific topics, and educational initiatives in conjunction with national universities. Our paper also includes information on how we handled cultural issues in the development and delivering of nuclear-cyber courses and how these courses have benefited the overall US-China confidence building process within the nuclear-cyber community.

Keywords: Nuclear-Cyber, Training and Education, Multicultural Exchange, United States, China
Gender

Male

Primary authors:  Mr ZONG, Bo;  LIU, Xiaojun;  Mr SPIRITO, Chris;  Mr NICKERSON, Charles

Presenters:  Mr ZONG, Bo;  Mr SPIRITO, Chris

Track Classification:  CC: Information and computer security considerations for nuclear security
How a Goal-Setting Approach Enables Effective Cyber Security Regulation

ONR is the UK’s independent nuclear regulator of nuclear safety, security and conventional health and safety at licensed nuclear sites in GB. This includes the existing fleet of operating reactors, fuel cycle facilities, waste management and decommissioning sites.

This paper will explore how our goal-setting approach enables effective cyber security regulation by placing clear accountability on dutyholders to demonstrate effective risk identification and management; agility to operate, improve and manage emergent risks; and to deliver a supportive organisational culture that recognises the risks associated with nuclear operations in a digitised, globalised, data-rich society. It will further look at the resource requirements for the effective regulation of cyber security in this outcome-focussed way.

Through an examination of examples generated through regulator-led duty holder-supported projects, it will illustrate how an enabling regulatory attitude has pushed forward understanding of good practice in the areas of:

Assessment of Assurance in the Operational Technology Domain
Partnering with a commercial provider, through a range of exercises we aimed to learn the extent to which a regulator could expect duty holders to conduct assessment of assurance in the operational technology domain. This included consideration of nuclear safety as well as organisational considerations. The approach considered built on good practice from other sectors, and incorporated the use of a threat led approach, and the mapping and testing of security controls, security systems and technologies that cover the various stages of the ICS cyber kill chain.

Use of Commercial Products to Compliment National Intelligence
Again with a commercial partner, with developed expertise in the area of commercial threat intelligence, we sought to understand from a regulatory perspective what expectations we could have on duty holder organisations in respect of their use of commercial products as a compliment to national intelligence. Through a series of experimental products we aimed to understand how effective and continuing access and consumption of up to date threat reporting that can be used to provide education, understanding and threat-informed mitigation strategies that specifically address the threat landscape for IT and OT in the organisation.

Resourcing Effective Regulation of Cyber Security
Using the evidence from the examples the paper will examine the developing need for competent resource in duty holder organisations, the regulatory body, and technical support organisations.

ONR’s own journey has seen it use contracted support from a commercial partner, as outlined previously, but additionally it has also recruited more than 10 new staff into the cyber security regulatory team over the past 4 years.

The paper will reflect on the journey from establishing the case for recruitment, through how recruited in a congested in-demand discipline, it will examines how we absorbing new recruits into a previously small team, finally it will look at how we are generating regulatory expertise, and managing the impact of increased capacity on the duty holder community.

Aim
The aim of this commentary is to provide other organisations seeking to enhance their capability with some considerations and lessons learnt.
State
United Kingdom

Gender
Male

Primary author: PARKHOUSE, Thomas
Presenter: PARKHOUSE, Thomas

Track Classification: CC: Information and computer security considerations for nuclear security
The security of research reactors and associated facilities are subject to regulatory assessment. This oversight is designed to ensure that the security system meets the required regulatory standards nationally and internationally. Though the intention of this is to prove that the systems will work against a defined adversary stated in regulations, it does not always be fully assured that it will work perfectly. The reasons could be the differing judgments on the effectiveness of certain measures and the fact that there is no one straight security measure that is likely to be wholly effective against that method and may not always be clear how other measures compensate for any such deficiency.

Some questions also arise because of the inevitable compromises that have to be made to accommodate conflicting priorities and because of the complexity of the systems involved. This starting point of the Methodology is, therefore, the existing regulatory framework, policies and guidance on which the security system is based. If, as a result of the Assessment, a security system is deemed insufficient it needs to be borne in mind that the failure may be, at least in part, in the Regulations not just their application.

This paper summarizes the work conducted by the authors working on the International Atomic Energy Agency (IAEA) Coordinated Research Project (CRP) on "Nuclear Security for Research Reactors and Associated Facilities (RRAFs)-J02006" and more specifically, Task 1. A Hypothetical Atomic Research Institute (HARI) was established to serve as the State’s premier nuclear energy research facility. HARI’s purpose is to build scientific expertise and capacity for the country. The Institute houses a research reactor facility, radioisotope production facility, fuel element fabrication facility, gamma irradiation facility, waste processing and storage facility, and administrative and facility support facilities. The study only considered the research reactor facility in the HARI. The main objective of this paper is to apply NUSAM results which are a performance-based methodological framework in a systematic, structured, comprehensive and appropriately transparent manner on Research Reactors and Associated facilities. The framework will be used to assess the nuclear security of nuclear and other radioactive materials, as well as associated facilities and activities within regulatory control. It is also to determine which methodology to apply, Simple, Complex or both, for RRAFs ensuring alignment between the NUSAM and RRAF CRPs and to develop "case study/ies" for RRAFs. The objective is to provide an environment for the sharing and transfer of knowledge and experience, and to provide guidance on, and practical examples of good practice in assessing the security of RAFFs and activities.

The intent of the Research Reactor Case Study was to evaluate the assessment methodology outlined as part of the NUSAM Methodological Framework. This case study focuses upon the use of a tabletop approach, which normally produces qualitative results, an alternate approach should include the use of a complementary tool for neutralization, which produces quantitative results. The tabletop proved adequate for the application of evaluating the effectiveness of the physical protection system at a research reactor facility. The following represents the conclusions of the working group team: 1) Tabletop prove useful, however with the absence of site-specific performance tested data, analysis would be difficult. 2) Tabletops have great impact if all stakeholders are involved and provide relevant information in the conduct of the tabletop analysis.
Gender
Male

Primary authors: RONMCCREA, CUSHNIE; Dr EK, David; Dr SHULL, Douglas; Dr KASSEM, KHATTAB; Ms JEANICE, Leach; Dr ATHANASIOS, SFETSOS; Dr ADU, Simon
Presenter: Dr ADU, Simon
Session Classification: Research Reactor Security
Track Classification: PP: Research reactor security
Implementation of the Borehole Disposal System for safe and secure management of Disused Radioactive Sources in Ghana.

Implementation of the Borehole Disposal System for safe and secure management of Disused Radioactive Sources in Ghana.
Eric T. Glover and Paul Essel
Radiation Protection Institute
Ghana Atomic Energy Commission

The Government of Ghana, through Ghana Atomic Energy Commission (GAEC) is implementing the Borehole Disposal System (BDS) developed under an International Atomic Energy Agency (IAEA) Regional Technical Cooperation Project in South Africa, for disposal of Disused Sealed Radioactive Sources (DSRS) as an end-point management option.

Radioactive materials have been in use in Ghana for more than six decades, mostly in the form of Sealed Radioactive Sources (SRS) for sustainable development. They are being used for diagnostic and therapeutic procedures in medicine, measurement and processing techniques in industry, irradiation techniques for food preservation, sterilization of medical products, research and teaching. The use of SRS generates Disused Sealed Radioactive Sources (DSRS) when they are no longer powerful enough for their intended purpose or when they fall out of use due to obsolescence of equipment or techniques. The DSRS require proper management to prevent any hazard to human health and the environment. Improper management of these beneficial devices have contributed to several incidents around the world that have resulted in serious injuries, death and extensive contamination of the environment. DSRS also present security concerns as the sources can be stolen and their radioactive materials used in radiological dispersion devices (dirty bombs) for acts of terrorism.

Very short-lived DSRS, i.e. those with half-lives of less than about one year, can usually be “decay stored” i.e. kept in storage for up to ten years until their activity has reached exemption levels when that can be disposed or recycled as non-radioactive waste. However long-term storage is required for long half-lives radionuclides such as Ra-226, which has a half-life of 1600 years.

Storage is an important radioactive waste management step, but long-term storage is not considered sustainable for hundreds to thousands of years and in many cases may represent a high-risk situation with regard to both the health hazard and the security threat posed by high activity long lived sealed sources due to food preservation, sterilization of medical products, research and teaching. DSRS also present security concerns as the sources can be stolen and their radioactive materials used in radiological dispersion devices (dirty bombs) for acts of terrorism.

The borehole disposal system (BDS), i.e. the disposal facility and the environment in which it is sited, entails the emplacement of conditioned DSRS in a relatively narrow diameter borehole, drilled to an intermediate depth and operated directly from the surface to provide safe and secure isolation of DSRS for thousands of years.

Safety and security measures have in common the aim of protecting human life and health, and the environment. Safety and security measures have therefore been designed and implemented in the BDS in an integrated manner so that security measures do not compromise safety and vice versa. The paper discusses the implementation of the BDS in Ghana as well as the safety and security features of the BDS.
State
Ghana

Gender
Male

Primary author: GLOVER, Eric Tetteh (Ghana Atomic Energy Commission)
Presenter: GLOVER, Eric Tetteh (Ghana Atomic Energy Commission)

Track Classification: CC: Nuclear safety and security interfaces
I. INTRODUCTION

The subject may hold our attention for several reasons; indeed:

- In economic terms, the Transport of Dangerous Goods sector is of interest to several stakeholders: packers; shippers; chargers; carriers; unloaders;

Thus, these goods allow us to feed to do x-rays and chemotherapy including tests in oil environment, etc..

- In practical terms, the need for this type of transport is well established; however, risks must also be controlled because of their dangerousness.

Since safety is everybody’s business, the public authorities propose for their part:

- to review the legal framework of this sector of activity in order to align it with the international context;
- to raise the awareness of the actors involved in this sector;
- to reinforce the reaction capacities of the competent services in the face of the related accidents, all the more so since, in view of the statistics of transport accidents available throughout the world, we have most of the accidentology in the transport of Dangerous substances with consequences for the population and the environment.

I will present the various Gabonese standards that govern the Transport of Nuclear and Radioactive Hazardous Materials, is anchored to that of the European Norms.

Gabon Law number 17/2013, fixed the regime of Safety, Security nuclear and radioactive, it states that, there is an authority at the head of the Agency. It issues all transport licenses from Radioactive and Nuclear sources.

Transport conditions are checked by operators through safety and security checks.

- the sender;

Ensures the packaging of sources and it must be homologated to the SGH (General Harmonized System) standard

He does the Labeling
It puts the General Harmonized System Pictogram sources
the symbol of the danger code
On this packaging it puts the name of the source, as well as the quantity and weight of the source.

He does the packing
He contacts the shipper, the carrier and the consignee and sends them all the information.

He must obtain the authorization of the head of the Radioactive and Nuclear Regulatory Agency

The carrier Must have source transportation protocol

He checks the packaging
Check the number of packages
Check that the safety sheet is full
Check the recipient’s address

Check that the recipient is waiting for the package

The approval of the head of the Radioactive and Nuclear Regulatory Agency
Driver trained in the transport and recovery of Radioactive and Nuclear sources
The driver has a driver's license and his authorization to drive the vehicle of Transport of the sources
Check the condition of the vehicle
There must be source signage documents
Have the category of sources to transport: If category 1 and 2, it will take a police or gendarmerie escort
Certificate of registration
Certificate of the technical visit
Insurance
Check the bill of lading, the number of packages, the nature of the product, the unique UN number ie the CAS or the trade name plus the nomenclature.
Checks Precautions, Shipper / Sender Manufacturer’s Call Numbers, Emergency Locator Numbers to Cross,
Permit to Move and Transport Product
The Vehicle must be homologated and have an approval compatible with the transported product
It must have the UN Pictogram on the back and on the sides
He must also have the documents of transport of dangerous materials, the safety cards in the truck (phone number of the person in charge of the sending company to seize in the event of an accident)
There must be a document that shows the nomenclature of the dangerous goods being transported, the maximum speed, the safety instructions and the instructions for driving, driving and schedules
The carrier is assisted by a security advisor and a commissionaire
The carrier must ensure that there is in his vehicles, the safety equipment
The Extinguisher
The holds
Cones or Triangle
The Lot of Edge
Personal protective equipment
-The charger
Train the loader using the loader
Have the protocol of loading loaders
Have chargers approved by the UN
Have a Transport Document for the transport of dangerous goods
Know the number of packages
Have a driver's license as a loader
Have the Training Certificate
The machine in charge must have the UN number
The receiver
This is where there is unloading
He must follow the Unloading Protocol
It has the same instructions as the charger
He is assisted by a security advisor and a commissionaire.

It must have sufficient storage depots to store the product during unloading.

All safety barriers must be operational.

For safety:

Safety plans are required for certain products and substances.

In the event of an accident, report to the facility classified to the environment, to the police, gendarmerie and customs; put a signage; alert the rescue quickly.

**State**

Gabon

**Gender**

Male

**Primary author:**  ALLAIN, Allogo

**Presenter:**  ALLAIN, Allogo

**Track Classification:**  PP: Transport of nuclear and other radioactive material: practices, challenges and regulatory issues
UK Experiences of Implementing Outcome Focused Security Regulation

UK Experiences of Implementing Outcome Focused Security Regulation

Historical Context

In 2003, the UK enacted the Nuclear Industries Security Regulations 2003 and the Office for Civil Nuclear Security (OCNS) was established under the Department of Trade and Industry as the enforcing regulatory body. Whilst these regulations are not inherently prescriptive in nature, the dominant culture of the time combined with a lack of capability and capacity within the regulator and regulated bodies led them to be implemented in a prescriptive fashion.

In 2007, OCNS was transferred to the Nuclear Installations Inspectorate, part of the Health and Safety Executive responsible for nuclear safety. It is now a fully integrated part of the Office for Nuclear Regulation, which was itself created by The Energy Act 2013. As part of this integration and to support a reinvigorated nuclear industry, ONR embarked on a transformation programme to move security regulation to a goal-setting approach.

Publication of National Objectives, Requirements and Model Standards

This paper will provide a brief overview of the history, but focusing on the timeline from the first stage of this transformation. This was the publication of the National Objectives, Requirements and Model Standards document in 2012 which placed an emphasis on meeting objectives and providing justification that arrangements were adequate rather than applying strict adherence to standards. However, the implementation review identified that a lack of stakeholder engagement during the development process, coupled with presence of directive language and specific security solutions meant that it was not fully successful in driving cultural changes required to support adoption of a goal setting approach.

Publication of Security Assessment Principles

ONR published the Security Assessment Principles (SyAPs) in 2017. In particular, it encouraged ownership, innovation and continuous improvement. Stakeholder engagement was fundamental to the development of this document. This ensured that the document’s intent and utility was fully understood by licensees, securing their support and allowing preparations to be made in anticipation of its publication.

SyAPs marked the end of the regulator publishing a suite of technical requirements for licensees to implement and instead provided a framework to assist in the assessment of arrangements based on the demonstration of meeting graded outcomes. It is tiered in structure and was developed with the intent of allowing dutyholders to adopt aligned, complimentary arrangements that would satisfy the expectations of both security and safety regulation concurrently. In removing any model standards, a key aim of SyAPs was to transfer risk and ownership for security to licenses and other dutyholder organizations, ensuring they are the controlling mind whilst encouraging innovation and efficiency through ONR’s adoption of an enabling approach to regulation.

In addition to the removal of technical standards, SyAPs significantly expanded regulatory expectations into strategic areas such as governance, leadership, competence management and supply chain assurance. It was also authored to allow publication in the interests of openness and transparency, assisting communication through widening the audience of people that would typically have access to security documentation.

Implementation
The journey towards implementing outcome focused regulation has been and continues to be extremely challenging. ONR has significantly upskilled its workforce to accommodate the new approach and a similar professionalisation of security is being witnessed within the industry, where increased ownership has also resulted in positive changes to culture.

This paper will expand on this operational experience, setting out the successes, learning points, short term gains and expected long term benefits.

State

United Kingdom

Gender

Male

Primary author: Mr SIMS, Matthew (Office for Nuclear Regulation)

Presenter: Mr SIMS, Matthew (Office for Nuclear Regulation)

Track Classification: CC: Implementation of national legislative and regulatory frameworks, and international instruments
Development of a Human Reliability Program for a Low Power Research Reactor Facility as Measure to Mitigate Against Insider Threat

Human reliability from security point of view is challenging because internal and external influences can negatively impact the reliability and trustworthiness of employees in an organization. As a result, employees with access, knowledge and authority who develop malevolent intent against a facility pose a serious risk. Although, the Nigeria Research Reactor-1 facility is a low power research reactor, like any other nuclear facility is not immune from such threats. Only recently, Nigeria has witnessed a wave of security threats coupled with the desire by terrorist to acquire nuclear and radioactive material, the reactor facility, needs personnel who can be trusted with this critical technology, hazardous nuclear and radioactive materials. While robust physical measures have been put in place at the reactor facility to mitigate external threats, internal threats are difficult to mitigate because of the difficulty in identification and detection of perpetrators. Therefore, it is critical that security programs such as the Human reliability program are developed for personnel who work in positions of trust. Human reliability Program is a security and safety program designed to ensure that individuals who occupy positions with access to certain nuclear material, facilities and programs meet the highest standard of reliability, trustworthiness, and physical and as well as mental suitability. In this paper, we describe the development of Human Reliability Program for a low power research reactor facility in Nigeria to mitigate against insider threat.

Keywords: Security, Safety, Insider, Threat, Reliability, Trustworthiness.

State
Nigeria

Gender
Male

Primary authors: Dr IBRAHIM, Yakubu Viva (Centre for Energy Research and Training, Ahmadu Bello University, Zaria-Nigeria); Mr LYNCH, Patric (Oak Ridge National Laboratory); Prof. HALL, Howard (University of Tennessee, Tennessee, USA); Prof. STAINBACK, Joseph Ruric (University of Tennessee, Tennessee, USA)

Presenter: Dr IBRAHIM, Yakubu Viva (Centre for Energy Research and Training, Ahmadu Bello University, Zaria-Nigeria)

Track Classification: PP: Insider threats
Nuclear security aspect of the new NRNU MEPhI master program for Rostechnadzor.

The possibility of malicious acts involving nuclear or radioactive materials remains a worldwide threat. Ensuring nuclear security (NS) is one of the main responsibilities of an operator of any facility using nuclear / radioactive materials, and should be regulated by the state. Accounting, control and physical protection of nuclear materials and facilities are the subject of regulation. A prerequisite for the implementation of a NS regime is the appointment of competent authorities, among which must be a safety regulatory authority.

The development of human resources is one of the challenges in maintaining the required adequate level of NS to prevent, detect and suppress malicious acts directed at nuclear materials. In practice, there is a permanent loss of qualified personnel due to career growth, retirement and administrative changes, which influences negatively on the readiness of NS tasks performing of government bodies. Further, technologies and procedures are developing at an ever faster with the introduction of new equipment and technologies.

Therefore, there is a need for qualified NS experts at the national level. It is very important that sustainable NS competencies are achieved and maintained in each country to ensure and enhance global security. This goal can be achieved through training and education at all levels and in all organizations and facilities dealing with nuclear technologies. Educated and trained personnel is needed for government bodies, nuclear and radiation facilities. The training and education institutions play an important role in this process.

The master’s educational program “Accounting, Control and Physical Protection of Nuclear Materials” was created at NRNU MEPhI in 1997. This was the first systematic training of specialists with higher education in NS in Russia. The program was designed for people with technical education (engineer or a bachelor’s degree) in relevant areas. In general, about 200 graduates were trained under this program, (including Kazakhstan, Belarus). In addition, the university has experience in training specialists under the joint program of Rostechnadzor and the NRC.

In May 2018, an agreement on scientific and technical cooperation was signed between NRNU MEPhI and the Federal Service for Environmental, Technological and Nuclear Supervision of Russia (Rostechnadzor). Rostechnadzor is the authorized state safety and security regulatory authority in the nuclear area in Russia.

The agreement framework covers a wide range of interactions, including the application of modern digital technologies for knowledge management, improving the methodological basis of educational area, the professional advanced training in the field of nuclear safety and security, Under this Agreement, a master’s program is being developed for training specialists for the Rostechnadzor in MEPhI. The wide experience of other educational programs in the field of nuclear security is used in developing this program. The area of competence will cover the most fully planned activities of Rostechnadzor employees:

1. Regulation of safety of nuclear power plants and nuclear research facilities.
2. Regulation of safety of nuclear fuel cycle facilities, nuclear power plants of ships and radiation hazardous facilities.
4. Supervision of accounting and control of nuclear materials and radioactive substances and physical protection.

The last point constitutes a very important activity in securing the NS. Therefore, the program features are the saturation of disciplines in the field of physical protection, accounting and control of nuclear materials. Including classes in laboratories. NS competence is planned to develop the following disciplines:

**Technical aspects of ensuring the nuclear non-proliferation regime:**

Properties of nuclear materials, increasing their security
International Nuclear Non-Proliferation Regime
National Nuclear Nonproliferation Safeguards
Methods of physical measurements of nuclear materials:
Destructive and non-destructive methods for determining the mass and isotopic composition.
Instruments and equipment, measurement quality control.

Accounting and control procedures for nuclear materials:
Physical inventory.
Seals, barcodes, etc.

Design and evaluation of the effectiveness of physical protection systems:
Basic project threats.
General principles of physical protection systems design.
Vulnerability analysis of nuclear sites.

Technical means of physical protection of nuclear materials:
Sensors and detection.
Physical barriers and delay systems.
Access control.

The implementation of this educational program will create a strengthened human resource in one of the key areas of state security.

References:
Interfaces between Nuclear Safety and Nuclear Security For Existing Nuclear Reactors

Nuclear safety and nuclear security measures have in common the aim of protecting human life and health and the environment from the harmful effects of ionizing radiation. Thus, both must be designed and implemented in an integrated manner to ensure security measures do not compromise nuclear safety and nuclear safety measures do not compromise security. If there are interactions between nuclear safety and nuclear security functions of technical systems, organizational and administrative measures including plant procedures in a NPP in operation and within or between regulatory authorities, it is called an "interface between nuclear safety and nuclear security" within the scope of this document.

To identify potentially relevant interactions of the interface between nuclear safety and nuclear security with a level of detail comparable to the level of detailed Safety Reference Levels for Existing Reactors, the following tasks have been performed:

(1) Identification of national and international nuclear safety regulations where an interface with nuclear security is present. On an international level, IAEA standards have been used as source of information.

(2) Identification of national and international security regulations where an interface with nuclear safety is present. On an international level, IAEA standards have been used as source of information.

(3) Evaluation of national and international experiences related to nuclear safety if an interface with nuclear security was identified.

(4) Evaluation of national experiences related to nuclear security if an interface with nuclear safety was identified.

(5) Identification of further sources of information with relevant input for the Task Force, e.g. results of activities performed by technical support organizations or other relevant authorities dealing with the interface between nuclear safety and nuclear security.

The interfaces identified with the previously introduced approach are described below. This report includes guidance for work in the field of nuclear safety or nuclear security to be aware of and take into consideration the effects of potential interfaces. Interfaces between nuclear safety and nuclear security are also relevant to consider for the licensee, competent authorities and for other stakeholders (e.g. technical support organisations). In addition it is intended to highlight the common aim of nuclear safety and nuclear security and to strengthen the arguments for nuclear safety and nuclear security experts to work together to achieve this aim.

State

Egypt

Gender

Male
Primary author: ELHAMY ISHAK TAWFICK, peter (Egyptian Nuclear and Radiological Regulatory Authority)

Presenter: ELHAMY ISHAK TAWFICK, peter (Egyptian Nuclear and Radiological Regulatory Authority)

Track Classification: CC: Nuclear safety and security interfaces
BUILDING NUCLEAR FORENSIC SCIENCE CAPABILITY IN GHANA: PROSPECTS AND CHALLENGES

Forensic science is the application of sciences such as physics, chemistry, biology, computer science and engineering to matters of law. Forensic science can help investigators understand how blood spatter patterns occur (physics), learn the composition and source of evidence such as drugs and trace materials (chemistry) or determine the identity of an unknown suspect (biology). Forensics play key role in the criminal justice system by providing scientifically based information through the analysis of physical evidence.

Ghana achieved a middle income economic status and has a sharp increase in the incidence of crime over the past eight years. The government responded to this challenge by teaming up with international bodies to resource existing crime-combating laboratories and agencies to deal with the menace.

The Criminal Investigation Department of the Ghana Police Service, which operates The Forensic Science Laboratory received a grant of £3 Million funding from the European Union to refurbish the Laboratory and expand its capabilities into a State-of-the Art Facility. The Facility is an ultra-modern forensic laboratory, the first of its kind in West Africa. The Laboratory is located in Accra and serves all the 651 police stations across the 10 regions of Ghana. Other forensic services including medico-legal pathology services have been provided to the Ghana Police Service by the Criminal Investigation Department (CID), public hospitals and the Ghana Standards Authority which operates a special drugs, cosmetics and forensic laboratory.

In July 2012, a Memorandum of Understanding was signed between the CID and e-Crime Bureau Inc., a cyber-security and e-crime investigation firm based in Accra, Ghana to train CID detectives and establish an e-Crime Lab at the CID Forensic Science Laboratory.

Following major advancements in forensic science within the past eight years in Ghana, forensic science education programs have been developed in some tertiary institutions to help train scientists in the field. The Department of Biochemistry and Biotechnology of the Kwame Nkrumah University of Science and Technology was the first to start a Master of Science (MSc) and Master of Philosophy (MPhil.) in forensic science in the 2014/2015 academic year. The University of Cape Coast has also commenced a 4 year Bachelor of Science (BSc.) degree in forensic science, and The University of Ghana is in the process of acquiring accreditation to run master of science degree programme in Forensic Science. Plans are far advanced to start training students in the field of Nuclear Forensics at the University of Ghana, in collaboration with the Ghana Atomic Energy Commission and the Nuclear Regulatory Authority.

In spite of these advancements, myriad of challenges continue to plaque the forensic science sector in Ghana. This presentation will seek to shed light on the forensic science facilities, capabilities, challenges and the interventions made by stakeholders in fighting crime and promoting forensic science in Ghana.

State
Ghana

Gender
Female

**Primary authors:** Dr ADU, Simon; Mr AKROFI, Samuel; Ms NKATIA, Alice; Dr KOFI, Afrifah

**Presenter:** Ms NKATIA, Alice

**Track Classification:** MORC: Nuclear forensics
Nuclear security for radioactive sources used in mobile devices for industrial applications in Argentina

The use of sealed radioactive sources in industrial applications, with different purposes, is a practice widely implemented in several facilities in Argentina. In this context, for nuclear security, it is of special interest due to their own characteristics, the case of sources used in mobile devices, such as equipment for industrial gammagraphy or well logging (Category 2 and 3 sources according to the classification of the International Atomic Energy Agency). In these cases, due to the geographic zones in which these practices are usually carried out, generally little inhabited and far away from the main urban centers, it is necessary that authorized operators travel long distances transporting these devices, which increases the vulnerability of the sources. This particular situation requires the elaboration and implementation of nuclear security plans that contemplate measures for transport (including transit stops and overnight) as well as for temporary storages in the field and during the practices (operation), considering a graded approach depending on the category of the radioactive source and the potential threat, and in depth defense for the different security functions of the system.

In Argentina, the Nuclear Regulatory Authority (ARN – Autoridad Regulatoria Nuclear) is the entity devoted to the regulation of the nuclear activities in the country, with competence in the areas of radiological and nuclear safety, safeguards and non-proliferation, and physical protection. The ARN is empowered to establish the regulatory standards within its competence, to license facilities and practices that use radioactive material as well as the personnel with safety relevant functions, and to control the activity (performing inspections and regulatory audits).

In this country, there are several companies which hold 74 operation licenses for industrial gammagraphy purposes, and 33 operation licenses related to the oil industry, 11 of which are licenses for well logging purposes (information updated to December 2018).

The objective of this work is to explain the current situation in Argentina related to nuclear security for radioactive sources used in mobile devices for industrial applications and the associated difficulty, describing the applicable regulatory framework and the use of international guidance, sharing the field exercises carried out in order to improve the interaction among the different actors involved in the activity, and proposing measures to be considered, aspects of the interface safety-security, good practices and recommendations, in order to strengthen the nuclear security of these practices, in a sustainable manner.

State

Argentina

Gender

Male

Primary authors: Mr RIVERO, Sergio (AUTORIDAD REGULATORIA NUCLEAR); Mr FERNAN-
DEZ, Alejandro (AUTORIDAD REGULATORIA NUCLEAR)

**Presenter:** Mr RIVERO, Sergio (AUTORIDAD REGULATORIA NUCLEAR)

**Track Classification:** CC: National nuclear security regulations
Enhancing Nuclear Security of Nuclear and Radiation Facilities from the perspective of Regulatory Enforcement and Inspection

Abstract
Nuclear powers plants are one of the most important nuclear facilities, are considered to be a safe, economically viable, sustainable and environment friendly power source for the socio-economic development of any country. Most of the embarking countries have established or are in the process of establishing their legislative and regulatory framework to assess and subsequently authorize nuclear security within the licensing framework for nuclear and radiation facilities. In order to maintain nuclear security, in each phase of the life cycles of nuclear and radiation facilities, at least the following shall be inspected by the nuclear security authority on a regular, scheduled basis in a manner specified. This study aim to enhance and improve the regulatory enforcement and inspection by addressing in national law and regulations clearly establish inspection rights of regulatory authority, training of inspectors to be qualifies, description of process for announced and unannounced inspections, development of procedures and launch improve and modification programmes designed to ensure that inspection services are carried efficiently and effectively, having respect to the costs for government in the delivery of inspection services and adapting the organisation of inspection services to utilise changes in technology and social organisation to achieve regulatory objectives. As well as the regulatory authority shall draw up an inspection plan containing inter-alia the subject matter of scheduled inspections, the period inspected, the timetable and means of the inspections, the criteria for inspections and other particulars defined by regulatory authority. Also perform a document review and identify discrepancies between the facility documentation and the national regulatory requirements, where verify documentary evidence exists to verify requirements defined in the licensee security plan and implementation procedures where regulatory staff categorizes these violations in terms number of levels or colour of severity to show their relative importance or significance.

The main targets for improvement and modification are generally to reduce the administrative loads and other obstacles, to improve the effectiveness of enforcement practices and therefore improve regulatory compliance – and in some cases to increase efficiency and thus decrease budgetary costs to governments. The improve of enforcement and inspections is as much about changing methods and culture as it is about reforming institutions organisational mechanisms and legislation. Finally, we recommended details to improve the regulatory enforcement and inspection of nuclear security for nuclear and radiation facilities.

State
Egypt

Gender
Male
Primary author: Mr HAZZAA, Mohamed helmy (Egyptian Nuclear and Radiological Regulatory Authority (ENRRA))

Co-authors: Dr SHABAN, Sameh; Dr EL-TAYEBANY, Rasha (Egyptian Nuclear and Radiological Regulatory Authority (ENRRA))

Presenter: Mr HAZZAA, Mohamed helmy (Egyptian Nuclear and Radiological Regulatory Authority (ENRRA))

Track Classification: CC: National nuclear security inspections: training of inspectors, development of procedures and managing findings
Experience of Cameroon on a case study related to the security of the orphan radioactive source

Sealed radioactive sources are used for a wide variety of purposes in Cameroon. A wide range of these sources or activities exist before the establishment and functioning of the Cameroon National Regulatory Authority. The main challenge of the Cameroon government through its National Regulatory Authority has always been to have knowledge on the radioactive source used under its territory. This can only be achieved by establishing a strong legislation and communication with the interested parties on the risk, safety and security of radioactive sources. This paper discussed experience of Cameroon on a case study related to the security of the orphan radioactive source found in the Sea Port of Cameroon. The source was discovered when dismantled the dredging of Yougwe. This radioactive source was used by the staff of this port without any knowledge on radiation protection and security of radioactive source. The discovered radioactive source was handled out of regulatory procedures by a foreign company. The actions to temporary secure this orphan radioactive source was undertaken by the National Radiation Protection Agency in collaboration with sea port authority. These activities include the training of staff on radiation protection, security of radioactive source, management of disused radioactive source, safe handling for transport and storage.

State
Cameroon

Gender
Male

Primary author: Prof. NDONTCHUENG MOYO, MAURICE (ANRP)
Co-authors: Dr SIMO, AUGUSTIN (NRPA); Dr NGUELEM MEKONGTSO, JILBERT ERIC (NRPA)
Presenter: Prof. NDONTCHUENG MOYO, MAURICE (ANRP)

Track Classification: PP: National accounting and control measures of radioactive materials
TERRIFFIC: Tools for the initial 30 minutes after a CBRNe incident

The time needed to assess the situation after a CBRNe (Chemical, Biological, Radiological, Nuclear, explosives) incident is critical to minimize the exposure of the public as well as first responders. This trade-off between speed, effectiveness and the safety of first responders during the first hours continues to be a major challenge today, after many years of operational and technological innovation. To complicate things even more for first responders, the situation is often highly dynamic due to many factors - especially if the incident involves terrorism: the presence of perpetrators in the crime scene and combination of the Radiological and/or Nuclear (RN) attack with a conventional attack; changing meteorological conditions; fragility of buildings damaged by explosions; the presence of a secondary Improvised Explosive Devices (IEDs) timed to explode after the arrival of first responders; the presence, and state, of victims; the reaction of the civil population etc. Hence the situational awareness must be dynamically updated, in particular swiftly taking into account the evolution of the radiation plume and determining the extent and severity of the contamination and the dimensions of the control zone. The aim must be to collect and to update information quickly whilst in parallel the responders prepare for intervention or are already intervening. This allows to greatly reduce the damage, suffering and costs caused by CBRNe incidents. Within the European TERRIFFIC project trials are ongoing to optimize the assessment process. The paper presents newest developments within the TERRIFFIC project to get optimal information to first responders in the initial 30 minutes after an incident. The concept involves radiation monitoring with unmanned vehicles (drones and robots). A comprehensive system of complementary, interconnected and modular software and hardware components will be presented. Advanced mixed reality technology will be leveraged to provide first responders with ad-hoc available and continuously updated information during operations.

The TERRIFFIC project brings together 10 European organisations, which work together to deliver an important step change in the effectiveness of first responders during the initial hours of a Radiological, Nuclear, explosive (RNe) incident. This will lead to reduced response times, less health and safety risks for the response teams, and less human intervention in the operation due to a higher number of automated processes and extended mobile detection capabilities.

State
Switzerland

Gender
Female

Primary authors: DAVATZ, Giovanna (Arktis Radiation Detectors Ltd); CHANDRA, Rico (Arktis Detectors); Dr GENDOTTI, Ulisse (Arktis Radiation Detectors Ltd); Dr PANIENLO , Marco (Arktis Radiation Detectors Ltd)

Presenters: DAVATZ, Giovanna (Arktis Radiation Detectors Ltd); CHANDRA, Rico (Arktis Detectors); Dr GENDOTTI, Ulisse (Arktis Radiation Detectors Ltd)
Track Classification: CC: Emergency preparedness and response and nuclear security interfaces
From theory to practice on physical security (the experience of GKTC)

GKTC is a part of the Ukrainian State System of training, retraining and advanced training of MPC&A specialists. During the years of activity GKTC has prepared and delivered about 300 national training courses on nuclear security. More than 4500 Ukrainian specialists of about 90 institutions and organizations of Ukraine have raised their level of skills at these training courses. In 2012 an Exterior Training Site “Complex of Engineering and Technical Means of Physical Protection System” (ETS) with central and backup alarm stations and training classroom was created. ETS is a unique site in Ukraine where GKTC staff can create situations in real time that may occur at the facilities as a result of social and political nature events. ETS is very useful for Ukrainian specialists because such training cannot be conducted at operational nuclear facility without reducing the security level.

In 2018 "NPP with PPS Elements” Interactive complex was created. The use of this complex during the training will stimulate creative activity and analytical thinking of the course participants and allow them to acquire the skills they need to perform during guarding and protection of nuclear facilities.

GKTC creates two new laboratories:
1. Computer Security Laboratory.
   This laboratory is created to solve the problems of providing computer security in the field of nuclear security of critical infrastructure facilities due to the growth of cyberthreats.
2. Radiation Control Laboratory.
   This laboratory is created for personnel of National Guard of Ukraine to train them in the use of dosimetric instruments and radiometers.

Programs of all training courses include from 30 to 60 % of total training time for practical and laboratory exercises.

State

Ukraine

Gender

Male

Primary author:  Mr DRAPEY, Sergiy (Institute for Nuclear Research)
Co-authors:  Mr GAVRYLIUK, Viktor (Institute for Nuclear Research); Ms ROMANOVA, Olena (Institute for Nuclear Research); Ms HAVRYLIUK-BURAKOVA, Anna (Institute for Nuclear Research)
Presenter:  Mr DRAPEY, Sergiy (Institute for Nuclear Research)

Track Classification:  CC: Role of Nuclear Security Support Centers to support and sustain
national nuclear security regimes
System Evaluation Methods in practice for insider mitigation

In ensuring nuclear security, addressing the issues of countering the insider threat is one of the most difficult.

The main elements of the physical protection system are the technical means: CCTV, access control, locks, radiation monitors, etc., for which you can develop management scenarios, service and support procedures, modernization and improvement programs.

In turn, counteraction to the insider threat includes analysis of the behavioral manifestations of each individual person, his emotional and mental state, motivation, up to his relationships in the family, with friends and colleagues.

This significantly complicates the process of developing countermeasures to the insider threat, as compared, for example, to countering the terrorist threat.

In this case, the classical measures of physical protection, such as perimeter fencing, checkpoints, perimeter lighting, etc., lose their effectiveness and are not able to counteract the insider threat.

The approaches to evaluating the effectiveness of measures taken to counter the insider also change.

Determining the time to overcome physical barriers becomes irrelevant and meaningless.

In this case, it requires the development of a completely different approach combining the functions of classical physical protection, digital technologies and cyber security, safety security and the assessment of the behavioral characteristics of workers.

The national operator of Kazakhstan for the extraction and processing of natural uranium, NAC Kazatomprom JSC, in its practice of ensuring nuclear security and countering the insider threat, attempted to combine these functions.

In terms of providing classical physical protection, access control systems, full-coverage video surveillance and alarm systems have been introduced.

In terms of integrating digital technology and safety security, systems such as SC - visualization of key production processes (>500), ERP - financial planning and accounting, MES - Production Management, APS - operational planning, LIMS - laboratory information system, EAM - service, spare parts, APCS - automated process control system. These systems are integrated into a unified data management system and are presented in the Situation Center of the headquarters of NAC Kazatomprom JSC. The data management system allows real-time monitoring of changes in the equipment’s normal operation mode and blocking the introduction of these changes in case of critical deviations, which significantly complicates the implementation of the task of the insider during sabotage.

In terms of evaluating the behavioral functions and reliability of the staff, digital technologies are also actively used. As part of the Government’s implementation of the Digital Kazakhstan strategy, various information about the employee on tax arrears, administrative fines, travel bans, registered business, being in the register of wanted persons, etc. is available on a single portal providing state services.

With the help of special IT-aggregators, the Security Service of NAC Kazatomprom JSC carries out inspections of workers, including through open accounts in social networks. Conducting these activities allows you to generate primary information about the employee before interviewing him in the course of the assessment of reliability.

All of these measures allow an assessment of the measures taken to counter the insider threat, identify vulnerabilities and work out ways to improve the overall security system of the enterprise.
State
Kazakhstan

Gender
Male

Primary author: Mr NIKHANOV, Eldar (NAC Kazatomprom JSC)
Co-author: Mr ALZHANOV, Bekzhan (NAC Kazatomprom JSC)
Presenter: Mr NIKHANOV, Eldar (NAC Kazatomprom JSC)

Track Classification: PP: Insider threats
drafting regulations on the transport security of nuclear and others radioactive materials: experiences of african states

The International Atomic Energy Agency (IAEA) recognizes that the drafting of regulatory text is the means of guaranteeing an adequate nuclear legal regime in order to preserve peace, health and security of populations. For the IAEA, the challenges are great and various. To this end, the IAEA provides constant support in the development of legal text in the sensitive areas of nuclear safety and security. one of these areas is the transport of nuclear and others radioactive materials. transport is unquestionably a phase where the security of materials is vulnerable and all measures must be taken to avoid malicious acts.

The development of regulations on the transport security of nuclear material and others radioactive materials requires the combination of several competences. It brings together both technicians and legal experts and must follow a clearly established procedure to ensure the acceptability of the final text. however, national authorities in Africa do not always have these skills and even when these skills exist, they often need support or assistance to be more effective.

In this context, the IAEA supports african countries in strengthening their regulatory framework for transport security of nuclear and radioactive materials. In this exercise, the IAEA uses its network of international experts to assist countries in developing or consolidating their texts through the Nuclear safety and Nuclear security department. This use of international experts, external to the countries has significant advantages in achieving IAEA objectives. Successful examples of such support exist particularly in african countries. Examples includes Burkina Faso, the Democratic Republic of Congo, Benin, Mauritania and Ghana.

The tree should not hide the forest, the successes garnered by this form of assistance made by IAEA should not obscure the difficulties that exist in certain countries and which remain important challenges for the different countries but also for the IAEA.

The purpose of this paper is to highlight the challenges of development of regulations for the transport security of nuclear and others radioactive materials in african countries. It allows to discuss the place of regional experts in the process of drafting national regulations. At last, it allows to highlight the difficulties that undermine the process.

Proposed outline
1. Introduction
2. The challenge of drafting national regulations on the transport security of nuclear and others radioactive materials
3. Assistance from International Atomic Energy Agency
4. Use of regional expertise under the assistance of IAEA
5. Role of regional expert in the consolidation of national regulations
6. Case examples of some african countries
7. Some difficulties encountered and recommendations to deal with
8. Conclusion

State
Burkina Faso

Gender
Male
Primary authors:  Mr SOMDA, SAABESELE JEAN AUGUSTIN; LIWANGA, Jacques

Presenter:  Mr SOMDA, SAABESELE JEAN AUGUSTIN

Track Classification:  PP: Transport of nuclear and other radioactive material: practices, challenges and regulatory issues
Investigation of Initial Alarms from Radiation Detection Instruments

Equipment used for monitoring and assessment of cargo and pedestrians at borders are mainly handheld detector devices. The Radiation Handheld Devices (RHDs) are moved around a material (this can be in a form of cargo or be carried by a person) suspected to be emitting radiation. These detectors then alarm when the emitted radiation exceeds the established natural background radiation level of the detectors. Front Line Offices (FLOs) are the first point of contact with these materials and base on the RHD alarm and its associated data FLOs must decide if the alarm is the result of some innocent material or whether a secondary inspection or other action needs to be taken. This decision is most of the time complicated and frustrating to FLOs. Some RHD alarm profiles are not easily interpreted, especially when concerned with the possible presence of nuclear and other radioactive material, as issues with traffic/pedestrian management, speed with which measurement are done, manipulation of the different phases of some RHDs, weather, possible masking or shielding, etc., all present challenges to FLOs when making their initial assessments. Because the vast majority of alarms are simply the result of naturally occurring radioactive materials (NORMs) moving through commerce, separating alarms possibly caused by nuclear and other radioactive materials from the alarm pool of mostly NORM can be quite difficult. Additionally, fatigue of the operator and the 90% likelihood of the presence of NORMs (because that is usually the case) create a situation where material out of regulatory control could pass through a border crossing without being duly investigated. The above mentioned CRP is aimed at developing a composed tool for frontline officer to aid them in their analyses of cargo containing characters of radioactive materials at border post. Thus all project counterparts including the some staff of the Nuclear Security Department of NRA are required to collect such data for expert analyses and the development of the tool. Data collection was carried out on about a 100 conveyances/containers covering all kind of commodities passing through the two selected borders. These included a seaport and an airport. Commodity and container information were taken during the period. Data collection duration was within an average of 15 minutes on all visible surfaces of the containers with a pager and an identifinder. All data was inputted into an excel data sheet to be transfer onto the IAEA data sheet to aid in the development of the analysis tool. The research work performed supported the development and implementation of the TRACE (Tool for Radiation Alarm and Commodity Evaluation) application and associated algorithms. No separate publication was performed or applicable at this time. Data recorded included dose rate reading from the RHDs, identified radioisotope and accompany x-ray scans for every container. This provided detailed information for various cargo commodities. Cargo selection was according to the arrival of containers at the scanner section. Per the deliverables in the detailed programme, data collection has been carried out on about a 1000 conveyances/containers covering all kind of commodities passing through the two selected borders. These included the Tema Sea port, Kotoka International airport (KIA) as well as Takoradi Sea port at the western region of Ghana. Commodity and Container information were taken during the period.

State

Ghana
Gender
Female

Primary authors: MENSAH, Ann (Nuclear Regulatory Authority); ADU, Simon; APPIAH, kwame (nuclear regulatory authority); AGBENORKU, Obed (Nuclear Regulatory Authority)

Presenter: MENSAH, Ann (Nuclear Regulatory Authority)

Track Classification: MORC: Detection technology development and performance testing
Consideration of Artificial Intelligence for Cybersecurity Aspects of I&C Systems

After two extended up and down periods in the historical development of Artificial Intelligence (AI) during the last decades, since a few years, many AI solutions have become inherent components in several industrial business domains. We will briefly analyze how AI came to be where it is now and what boundary conditions have to be met in order to be able to apply AI. Yearly AI competitions allow for an outlook towards what performance the AI solutions are heading to. We will look at how AI is considered for security aspects in Industry 4.0 and how this can be applied for the nuclear domain, especially for Safety I&C, Operational I&C and Electrical Power Systems (EPS).

According to our focus, we will indicate what types of Machine Learning (ML) can be applied and what key security challenges have to be considered. The key AI supported concepts that will be addressed include: identification and authentication with AI support, AI supported anomaly detection in data streams and AI based identification of potential malware.

Beyond these AI based technologies for the implementation of selected security control, in two main sections we will address the genesis of new attack vectors through AI and the use of AI to improve the resilience of Safety I&C, OT and IT environments against sophisticated attacks.

Finally, we will also address the integration of AI approaches with traditional approaches from implementing and validating security controls and for attack tree analysis. This is an ongoing development where decisions on the effort for supervised Machine Learning (identification of representative vectors, tagging of artefacts, tagging of relations) or unsupervised ML has to be balanced with the effort for validating the results obtained via involved AI algorithms. With a focus on security testing the validation of representativeness and coverage of the AI based results remains an important challenge for ongoing R&D. The strength of the AI supported protection may have an impact to nuclear safety (due to potentially remaining residual risks), a topic that will be outlined but not elaborated in detail in this paper.

State

Germany

Gender

Female

Primary author: Ms BEN ZID, Ines
Co-authors: Ms LOU, Xinxin; Dr WAEDT, Karl
Presenter: Ms BEN ZID, Ines

Track Classification: CC: Information and computer security considerations for nuclear security
Advancing good practice: The work of the World Nuclear Association’s Security Working Group

The World Nuclear Association is an international trade body representing the global nuclear industry, including major reactor vendors, nuclear power plant operators, nuclear fuel suppliers and uranium miners, engineering, construction and waste management companies, along with professional service and transport providers. Its working group on fuel cycle security was reorganized in 2018 to better reflect member views and outputs from the Nuclear Industry Summit series held alongside the Nuclear Security Summits 2010–2016.

Whilst nuclear security is ultimately a State responsibility and an integral part of a State’s national security, licensed nuclear operators are responsible for ensuring that their facilities and materials are protected physically and that their technology and data are secure in accordance with legal and regulatory requirements. The global nuclear industry is committed to effective security and to continual improvement through the exchange of best practice, personnel training and regular review of plans and measures. The World Nuclear Association’s working group on security has adopted an agenda to examine a number of key areas: mitigating insider threats, cyber-security, the safety-security interface and culture, and to learning from other industries in order to establish good practice in corporate governance and communication with regulatory bodies and civil society.

This paper will inform on the progress made in these areas within the context of the changing security and market environment. It will offer suggestions on how the civil nuclear industry can work at the national and the international levels with governments, regulatory bodies and international organizations including the International Atomic Energy Agency to foster effective and efficient security within nuclear energy programs in established and embarking countries to engender a high level of stakeholder confidence.

State
United Kingdom

Gender
Male

Primary author: Mr KASER, Greg (World Nuclear Association)
Co-author: Dr HOWSLEY, Roger (World Institute for Nuclear Security)
Presenters: Mr KASER, Greg (World Nuclear Association); Dr HOWSLEY, Roger (World Institute for Nuclear Security)

Track Classification: CC: Contribution of industry to nuclear security
Implementation of Thailand’s Integrated Nuclear Security Support Plan (INSSP)

Thailand’s INSSP was developed in 2009 based on the findings and recommendations of IAEA team experts, the first review was in 2014 with the support of IAEA. Over the years, the Office of Atoms for Peace (OAP) continued to work on INSSP, as well as coordinate with the relevant authorities until Thailand’s legal instrument i.e. the entry into force of Thailand Nuclear Energy for Peace Act, B.E. 2559 (2016) provided the basis to comply with international security obligations. This instrument enables Thailand to move forward in further strengthening nuclear safety security and safeguards. Therefore, Thailand’s INSSP was reviewed again at the National meeting on INSSP review in September 2017, the purpose was to update INSSP status as well as to identify additional areas of nuclear security needs and gaps for the INSSP review mission with IAEA experts in November 2017.

Thailand’s INSSP was finalized in a constructive meeting that took place at the OAP from 6 - 10 November 2017 that involved the participation of relevant Thailand authorities and a team of experts from the IAEA Division of Nuclear Security. The valuable advice and suggestions were given by IAEA officers, Mr. David Smith, Mr. Fei Liu, and Mr. Gerhardus Liebenberg, as well as invited expert Dr. Nguyen Nu Hoai Vi to finalize Thailand’s INSSP. After that fruitful meeting, Thailand’s INSSP was approved officially on 10 April 2018. During end of April 2018, Mr. Raja Abdul Aziz Raja Adnan, Director of the Division of Nuclear Security, visited Thailand and had the opportunity to discuss the implementation of the approved Thailand’s INSSP in detail with OAP.

The approval of Thailand’s INSSP enables all stakeholders such as IAEA or Donor Countries to plan and coordinate activities from both technical and financial viewpoints to fulfill needs and identify gaps in INSSP document. The first implementation period focused on the areas of Threat and Risk Assessment as well as Response.

In the area of Response, nuclear forensics was highlighted and initial discussion about potential Practical Arrangements (PA) between The International Atomic Energy Agency and Office of Atoms for Peace on Cooperation in the Area of Nuclear Forensic Science was first suggested by Mr. David Smith during the INSSP Review Mission held at OAP in November 2017. The main purpose of such a PA is to facilitate and institutionalize further cooperation in the area of nuclear forensics. Furthermore, IAEA will provide assistance through Expert Mission on strengthening technical capabilities of the OAP nuclear forensics lab in 2019. Other activities supported by IAEA were also organized in the area of response e.g. National Workshop on National Response Plan for Nuclear Security Events.

In the area of Threat and Risk Assessment, Thailand updated the Design Basis Threat during a National DBT workshop in 2018 assisted by IAEA. Additionally, Thailand also organized the National Workshop on Nuclear Security Information Management System to review the status of their nuclear security infrastructure through INSSP document.

After the implementation of INSSP, nuclear security activities in Thailand became widely recognized at the policymaker level, which is the key driving force for sustaining nuclear security in the country. The successful implementation of INSSP can assist the State in developing and maintaining a strategy on enhancing nuclear security. In this paper, the implementation of Thailand’s INSSP will be discussed in details.
Gender

Female

Primary author: RUEANNGOEN, AREERAK (Office of Atoms for Peace, Thailand)

Co-authors: Ms THONG-IN, Saowaluck (Office of Atoms for Peace); Mr PHAUJKKACHANE, Paphon (Office of Atoms for Peace, Thailand); KASIWATTANAWUT, Haruetai (Office of Atoms for Peace, Thailand); Ms CHANGKRUENG, Kalaya (Office of Atoms for Peace, Thailand); Mrs SRIJITTAWA, Ladapa (Office of Atoms for Peace, Thailand); Ms MUNGPAYABAN, Harinate (Office of Atoms for Peace, Thailand)

Presenter: RUEANNGOEN, AREERAK (Office of Atoms for Peace, Thailand)

Track Classification: CC: Identification of national needs through the development of an Integrated Nuclear Security Support Plan
Advanced methods for radioactive and nuclear (RN) materials detection and characterization

In the global effort to reduce proliferation risks, and misuse, of radioactive and nuclear (RN) materials, effective and affordable technologies are required to improve areas identified by diverse national nuclear regulatory agencies. Canadian Nuclear Laboratories (CNL) is engaged on many fronts to enhance cutting-edge techniques and methodologies to address evolving national and international threats in nuclear safety and security. Examples of on-going initiatives at CNL in the area of detection of RN materials include: improvements in detection capabilities at borders by increasing portal monitors sensitivity and refining decision-making algorithms, set-up of a new test facility for evaluation of radiation detectors employing special nuclear material, development of high-level and dedicated training for front line officers involved in RN detection, study of active neutron and gamma-ray interrogation methods, employment of stand-off radiation detectors (e.g., large area neutron detectors, muon tomography) to locate radioactive materials and support the monitoring of fissile material to prevent diversion, detection of shielded RN materials in cargo containers by integrating several detection technologies, and development of innovative technologies such as liquid argon, liquid scintillator and dual PVT panels enabling gamma-neutron discrimination. In this talk we report on several efforts underway at CNL to strengthen nuclear safety and security program by investigating optimum ways to passively and actively interrogate suspected object for RN material detection and characterization.

State

Canada

Gender

Primary author:  Dr BENTOUMI, Ghaouti (Canadian Nuclear laboratories)

Co-author:  Dr SUR, Bhaskar (Canadian Nuclear Laboratories)

Presenter:  Dr BENTOUMI, Ghaouti (Canadian Nuclear laboratories)

Track Classification:  MORC: Detection technology development and performance testing
INSSP Implementation in Lebanon: Ten years of achievements and the way forward

The Government of Lebanon requested an INSerV mission in 2006 for evaluating the nuclear security measures that need to be taken in Lebanon for implementing a comprehensive scheme for combating the illicit trafficking of radioactive and nuclear material and to enhance the physical protection relevant to radiological facilities.

The first integrated Nuclear Security Support Plan, drafted in 2008 and endorsed in 2010 by all concerned national bodies with the assistance of the IAEA (Nuclear Security Division) was based on the recommendations and suggestions of the INSerV mission.

The INSSP of Lebanon was updated in 2012, 2016 and in 2019 and it covers legal and regulatory framework, prevention, detection, emergency and response and HRD.

The implementation of the INSSP in Lebanon will be presented in a comprehensive manner showing the involvement of all concerned national stakeholders, the national official structure created for the better effectiveness and efficiency in Inter-Agency coordination and cooperation, that is needed for the smooth efficient and sustainable implementation activities related to the INSSP document.

The achievement in establishing nuclear security units, structure and capacities within the national stakeholders (Lebanese Army, Internal Security Forces, Customs, General Security, Civil Defense, Red Cross, LAEC…) and their role in the nuclear security national scheme will be presented and discussed with a highlight on the achievement related to the repatriation of category I and II disused radioactive sources, effectiveness of the control of illicit trafficking of radioactive and nuclear materials and the management of radioactive waste from security point view at the national level.

State
Lebanon

Gender

Primary authors:  Dr NSOULI, Bilal (Director of the Lebanese Atomic Energy Commission-CNRS); Dr ZAHRAMAN, Khaled (Head of Nuclear Security and Radiological Emergency Department - Lebanese Atomic Energy Commission- CNRS); Mrs ASSI, Muzna (Research Assistant- Lebanese Atomic Energy Commission)

Presenter:  Dr NSOULI, Bilal (Director of the Lebanese Atomic Energy Commission-CNRS)

Track Classification:  CC: Identification of national needs through the development of an Integrated Nuclear Security Support Plan
Border Monitoring Equipment Evaluation Best Practices Workshop

The Border Monitoring Working Group (BMWG) was established in 2006 by the International Atomic Energy Agency (IAEA), European Union (EU) and United States (US) to share information for the purpose of harmonizing border monitoring activities in the areas of radiation detection equipment deployment, training and sustainability. Such coordination prevents the duplication of efforts, exploits organizational strengths and maximizes the impact of limited resources. Since its establishment, the BMWG has proven to not only be an effective tool for avoiding duplication and maximizing resource targeting, but also through a subordinate Technical Working Group to serve as a forum to address common technical concerns while jointly developing capacity building tools.

An important issue that the BMWG tackles is ensuring that radiation detection equipment capability and performance is commensurate with end-user needs and constraints. In fact, the group is currently active in the testing of the radiation-detection equipment that is used in EU, US, and many IAEA Member States receiving assistance from BMWG donor members. Recently, BMWG participants from NSDD and the IAEA developed and carried out an IAEA workshop to share technical information that might help partner countries build their own capability for evaluating radiation-detection equipment. The workshop focused on best-practice information sharing on the testing, evaluation, and development of test methods for radiation detector performance characterization. The inaugural session of The Testing and Evaluation of Spectrometric Handhelds Workshop was held at IAEA’s Seibersdorf Laboratory outside of Vienna, Austria, 25-29 June 2018. The workshop included seventeen participants from nine countries: India, Poland, Korea, China, Ukraine, Hungary, Indonesia, Malaysia, and Thailand. Additionally attending were: seven facilitators from the U.S. Department of Energy Office of Nuclear Smuggling Detection and Deterrence (NSDD), four facilitators from IAEA, three observers from BMWG and members from Germany, France and the United Kingdom.

The principles and practical aspects of developing and implementing radiation detection test methods were effectively delivered through scenario-based activities and discussion. The participants moved through four process-related technical scenarios:

1. Collection of high-precision spectral measurements of various sources, including HEU, to provide input data for the Modeling and Simulation exercises;
2. Modeling and simulation activities focusing on the use of a newly-available Replicative Assessment of Spectroscopic Equipment (RASE) software product enabling realistic, simulated instrument algorithm testing;
3. Measurement of the probability of false identification rates for the RIIDs being tested; and
4. Measurement of the probability of identification as a function of flux (or distance), along with demonstration of testing automation.

The scenario approach using small groups with hands-on activity proved to be a very practical approach to meeting the workshop objectives.

Outcomes from the well-received workshop included sharing previously collected test data, the execution of practical performance test methods, and the distribution of tools that the nine participating Member States immediately began applying to their nuclear security efforts. This workshop is a successful example of how the BMWG collaboration and relationships continue to be well positioned to meet the needs of global security through practical, beneficial assistance, in an agile manner that is also responsive to emerging trends based on an evolving understanding of capabilities and gaps.
State
Other

Gender
Male

Primary author:  Mr DIMMERLING, Paul (US DOE NNSA)
Co-authors:  Dr MASSEY, Charles (IAEA);  Mr HARRIS, Tyrone (IAEA);  Dr ANDERSON, Stephen (Los Alamos National Laboratory);  Mr DEMBOSKI, Mike (Pacific Northwest National Laboratory)

Presenter:  Dr MASSEY, Charles (IAEA)

Track Classification:  MORC: Detection technology development and performance testing
Nuclear security of nuclear fuel cycle facilities: mains threats and scenarios approach.

Under the topic for technical session appendix: “Nuclear security of nuclear fuel cycle facilities: emerging technologies and associated challenges and complex threats.”

One of the objectives pursued within the regulatory function is to ensure that nuclear materials are used only for peaceful purposes and prevent and deter unauthorized access to such materials that could cause hazardous situations or harm.

The Nuclear Regulatory Authority is the Argentine national body in charge of the regulatory affairs regarding radiological and nuclear safety, physical protection and security, safeguards and non-proliferation issues, and, in addition, its mission is to advise different State Branches in matters of its competence.

The aforementioned objective related to security is in charge of the Control of Safeguards and Physical Protection Division, and they fall within the Argentine Regulatory framework, under the regulations AR 10.13.1 and AR 10.13.2.

Regarding the nuclear industry and its facilities, the nuclear fuel cycle comprises several stages, which involve numerous industrial processes of varying complexity. Each of those stages face a variety of threats depending on which is its relative position in the nuclear fuel cycle.

While it is true that all nuclear facilities are designed to comply with strict standards of nuclear safety and security in order to protect the public and the environment against consequences of a nuclear accident or specifically malicious acts, it is important to consider that not all facilities have the same vulnerabilities or attractiveness, from the nuclear security perspective. Definition of threats associated to a nuclear facility devoted to energy production, as a nuclear power plant, could be significantly different to those threats definitions connected to a uranium enrichment facility, for example.

The aim of this paper is to discuss about the main threats faced by each of these stages and the main measures referred to physical protection and nuclear security. The way in which these measures should be implemented in order to prevent and mitigate possible theft and sabotage scenarios that facilities could face, focusing on the need to design adequate security systems according the activity carried out and taking into account defense in deep and gradual approach concepts.

Besides regulations and requirements, an important aspect in the success of physical protection measures, is the organizational commitment, which required a coordinated approach amongst security managers, operators, and regulators, in order to ensure an effective implementation and fulfill the regulatory requirements for which the system was designed. A short discussion about this subject will be also included in this work.

State
Argentina

Gender
Female
International Co... / Report of Contributions

Nuclear security of nuclear fuel cycle facilities: emerging technologies and associated challenges and complex threats

Primary author: Ms GORDILLO, Mariana Elizabeth (Autoridad Regulatoria Nuclear)
Co-author: Mr BOTIGLIERI, Eduardo (Autoridad Regulatoria Nuclear)
Presenters: Ms GORDILLO, Mariana Elizabeth (Autoridad Regulatoria Nuclear); Mr BOTIGLIERI, Eduardo (Autoridad Regulatoria Nuclear)

Track Classification: PP: Nuclear security of nuclear fuel cycle facilities: emerging technologies and associated challenges and complex threats
Sustainable the Border Monitoring Activities in Thailand Program

In 2014, the Border monitoring activity in Thailand project was initiated by the supporting from the European Commission, Joint Research Center (JRC) Ispra, Institute for Transuranium Elements (ITU). The Office of Atoms for Peace (OAP) is responsible for the implementation of this project. The purpose of this project is to support the organization in charge of the fight against illicit trafficking of nuclear and radioactive materials in the Kingdom of Thailand. This support will cover the deployment of radiation equipment as identified together with the OAP and the end users and the provision of corresponding training to the services involved. The deployed radiation detection equipment is Personal radiation detector, Radiation Identification Device and High Purity Germanium Detector. Those instruments were delivered to Thai Customs, Thailand Post, Royal Thai police (Forensic Science Police), Immigration Bureau, Airport Authority of Thailand and Bangkok Port Authority.

OAP is the competent authority which takes responsibility for training the end users on the development and practices of the procedures to detect and respond to radioactive and nuclear material out of regulatory control. Follow up the project, OAP provided the Memorandum of Understanding (MOU) with the end users to a central role and coordinate with all the end users and to ensure the achievement of this mission. OAP organized the yearly training on the National Front-Line Officers Training and Standard Operating Procedure Workshop on Radiation Detection and Response at Borders with the experts from IAEA, US DOE, and EC-JRC. Over the years, the awareness of nuclear security was widely recognized to the relevant authorities involving in the nuclear security aspect. Then again, the succeed from this strategy is the driving forwards on strengthening nuclear network in the country.

After the project has been finished successfully, hand-held equipment was exploited and routinely used to detect and respond to the cases of illicit trafficking of nuclear and radioactive materials out of regulatory control. Front-line officers have been trained for the proper use of the delivered equipment. Moreover, end users have received trained and also ready to provide training to others for better sustainability.

The purpose of this paper is to review the beneficial on the border monitoring activities in Thailand and the strategy on sustaining the mission, as well as the radiation monitoring methodology at the border by customs, police or other law enforcement bodies on the radiation monitoring illicit trafficking of nuclear and radioactive materials out of regulatory control at border crossing facilities.

State
Thailand

Gender
Female

Primary author: Ms CHANGKRUENG, Kalaya (Office of Atoms for Peace, Thailand)
Co-authors: Ms THONG-IN, Saowaluck (Office of Atoms for Peace); Mr PHAUKKACHANE, Papphon (Office of Atoms for Peace, Thailand); Mrs SRIJITTAWA, Ladapa (Office of Atoms for Peace, Thailand); RUEANNGOEN, AREERAK (Office of Atoms for Peace, Bangkok, Thailand); MUNGPAYABAN, Harinate (Office of Atoms for Peace); WITITTEERANON, Arug (Office of Atoms for Peace, Thailand)

Presenter: Ms CHANGKRUENG, Kalaya (Office of Atoms for Peace, Thailand)

Track Classification: MORC: Building and maintaining nuclear security detection architecture
International Symposium on Transport Security of Nuclear and other

Background

There are over 50 countries that have either nuclear power programs or research reactors which possess nuclear material and virtually all IAEA Member States possess and use other radioactive material, e.g. radioactive sources for medical, industrial and other non-nuclear applications. During the life-cycle of these materials, safe and secure transport is required. Transport of these materials takes place in the public domain outside of secured facilities, often involving international transfers, multiple national and international stakeholders, and multiple security interfaces that must function seamlessly for continuous and effective security. With tens of millions of shipments of nuclear and other radioactive materials taking place all over the world annually, security during transport is one of the most complex aspects of the physical protection of these materials.

Discussion

As an outcome of the Fourth Nuclear Security Summit of 2016, held in Washington D.C., the Governments of Australia, Canada, Czech Republic, Finland, France, Hungary, Italy, Japan, Kazakhstan, Morocco, Spain, the Republic of Korea, Thailand, the United Kingdom, and the United States reaffirmed through INFCIRC/909 their will to further improve the overall security in the transport of nuclear and other radioactive materials. With this goal in mind, they expressed their commitment to further exchange national practices with other countries through the IAEA and the Global Initiative to Combat Nuclear Terrorism (GICNT). They also committed to actively support the IAEA as the central organization for coordinating activities and developing guidance documents, and support the GICNT and the Global Partnership Against the Spread of Weapons and Materials of Mass Destruction in developing and implementing its nuclear transport security activities, both of which address the commitments regarding nuclear transport security coming from the Nuclear Security Summit 2016.

In an effort to continue the momentum from the Nuclear Security Summit, the Government of Japan, in cooperation with the Integrated Support Center for Nuclear Nonproliferation and Nuclear Security of Japan Atomic Energy Agency (ISCN/JAEA), will host the International Symposium on Transport Security in November 2019. With over fifty countries invited to attend, the purpose of this event is to exchange and promote good practices in several topical area sessions related to the security of nuclear and other radioactive material in transport, such as Laws and Regulatory Framework, Physical Protection Systems, Response Actions, and Insider/Information Security. The Symposium intends to build support for international transport security and encourage IAEA Member States to actively work regionally and internationally with the IAEA’s transport security programme through the practical implementation and incorporation of IAEA Nuclear Security Series recommendations and guidance into their national frameworks for transport security. From these sessions, it is the host’s intent to detail a recommended path forward for future engagements in the security of nuclear and radioactive material in transport.

This paper will discuss the Symposium’s outcomes and highlight the forward momentum made by both signatories and non-signatories for the strengthening of all the critical elements of a State’s transport security regime, including physical protection systems, insider threats to the nuclear and radioactive material supply chains, planning and capabilities for law enforcement response to malicious transport security events, and employment of technology to address critical vulnerabilities to the transport of nuclear and other radioactive materials.

State

May 9, 2020

Page 506
Japan

Gender

Female

Primary authors: NORO, Naoko (Japan Atomic Energy Agency); Mr ABYEYTA, Brian (National Nuclear Security Administration); Mr DUHAMEL, David A. (Oak Ridge National Laboratory); Ms CROFT HOLT, Katherine (US DOE/NNSA)

Presenters: NORO, Naoko (Japan Atomic Energy Agency); Mr DUHAMEL, David A. (Oak Ridge National Laboratory)

Track Classification: PP: Transport of nuclear and other radioactive material: practices, challenges and regulatory issues
A NEW GENERATION OF RADIATION PORTAL MONITOR AND ITS FUTURE EVOLUTION

Radiation Portal Monitors (RPMs) play a key role in Nuclear Security applications for almost two decades. They enable to ensure on-line monitoring and guarantee the safety at borders or in critical infrastructures like big ports. The need for being able to rapidly detect gamma and neutron signatures is crucial for preventing illicit trafficking of radioactive sources or Special Nuclear Material (SNM) as Weapon Grade Plutonium (WGPu), potentially involved in dirty bombs or nuclear devices. Because of the worldwide demand related to Nuclear Security applications, a strong R&D effort was made for finding 3He free solutions for neutron detection.

For several years, CEA LIST led an intense R&D activity on the RPM topic, mainly carried out in the frame of different European projects and also with strategic industrial partnerships. The choice was made by the laboratory of focusing on solutions based on large size plastic scintillators. The latter is by definition not initially well adapted to radionuclide identification or to neutron detection, two essential features for Nuclear Security controls. Main reasons are low density, close to 1, low Zeff and non-intrinsic ability of standard plastic scintillators for discriminating neutrons and gamma-rays. For overcoming these limitations, an intense work was carried out by our laboratory to develop several configurations able to detect neutrons with a sufficient efficiency for being compliant with the ANSI 42-35 standard and also to develop algorithms able to provide a robust radionuclide identification. These developments were started in the frame of the FP7 SECUR-ED project at the beginning of the 2010’s, focusing on configurations combining several pillars working in coincidence mode. RPM developments were pursued through the FP7 SCINTILLA project which was mainly focused on performance benchmark for passive systems compared to reference standards. Finally, the 42 month Horizon 2020 C-BORD project (2015-2018) enabled to move a step forward on this topic, giving a unique opportunity for deploying such systems in different European borders and ports.

In this article, we will first make a review of the key developments carried out by CEA LIST in the frame of previous European projects (SECUR-ED, SCINTILLA, C-BORD). Then, we will make a focus on our most recent RPM developments, developed in close partnership with a Nuclear Industrial company. We will especially insist on our latest results obtained using this system, especially those related to radionuclide identification in complex cases. Finally, we will introduce future developments planned by CEA LIST in the framework of RPM developments.
Presenter: CARREL, Frédérick (CEA LIST)

Track Classification: CC: Contribution of industry to nuclear security
New neutron and gamma detection capacity for preventing illicit trafficking of nuclear and radioactive material

Neutron emission is a typical signature from the presence of nuclear material (particularly uranium and plutonium isotopes that may be potentially involved in illicit trafficking of material out of regulatory control - MORC). Certain sources like 241Am Be or 252Cf have a significant neutron component and could be potentially used in the manufacture of dirty bomb.

The measurement of the neutron signature is therefore a major objective from the point of view of nuclear security, in order to prevent illicit trafficking of nuclear and radioactive material. Neutron detection is usually performed using 3He counters, sensitive to thermal neutrons (effective cross section of about 5400 barns for neutrons with energy close to 25 meV). Knowing that most of the neutrons to be detected are fast neutrons (emission according to a Watt spectrum for the isotopes undergoing spontaneous fission, average energy of the order of 2 MeV) and with 3He detectors it’s necessary to add a moderator (generally polyethylene) in order to optimize their detection sensitivity.

Since 2010, the strong demand for 3He on the nuclear security market has led to a shortage and a very significant increase of its price. For around eighteen years, research on credible alternatives to 3He, in terms of cost and detection efficiency, has been a major challenge for the research community. Numerous technologies have been studied: non-exhaustively, mention may be made of CLYC-type inorganic scintillators sensitive to thermal and fast neutrons, liquid scintillators and finally plastic scintillators.

On this specific problem of neutron detection, the CEA has focused its research for several years on solutions based on plastic scintillators, standard and modified.

The use of chemically modified plastic scintillators, thanks to the doping of our plastic scintillators by an organolithium complex, allows the detection of fast neutrons, thermal neutrons and gamma. This subject is studied as part of a CBRN-E counter terrorism research program aimed at developing a prototype of a fast neutron / thermal neutron / gamma discriminating handle detector. This new detector, allowing a triple discrimination, has been integrated in a measurement system in order to give the capacity to detect in the same time neutron and gamma emission to characterize for example a suspicious package.

In this article, we will present this new system developed and carried out by CEA LIST, we will also describe its associated features. Then a focus will be made on the use of this type of system and latest results obtained during an experiment in the field.

State

France

Gender

Primary author: BOUDERGUI, Karim (CEA List)
Data Analytics Supporting Provenance Assessment of Irradiated Nuclear Fuels

Nuclear forensics provides the ability to analyze radioactive and nuclear (RadNuc) material for the purposes of supporting the broader investigation of a nuclear security event. A comprehensive nuclear forensics capacity requires a capability to characterize and assess the provenance of materials discovered or seized from outside of regulatory control. The Government of Canada’s provenance assessment capability is supported, in part, through the Canadian National Nuclear Forensics Library (NNFL) program, which is led by the Canadian Nuclear Safety Commission (CNSC). The Government of Canada’s NNFL catalogues information and data about RadNuc material under Canadian regulatory control. The list of material groups captured under the Government of Canada’s NNFL framework includes irradiated nuclear fuels.

Characterization of nuclear fuels through post-irradiation examination has been historically focused on collecting and interpreting data and information for the purposes of supporting reactor engineering design, performance and safety applications. Similarly, the suite of codes and analysis tools has been, with some exceptions, primarily oriented towards these same applications. This work exploits the multitude of reactor engineering-focused spent fuel data sets and modelling tools for nuclear forensic purposes. The approach uses industry standard reactor physics codes to compute the nuclide composition as a function of burnup for various nuclear fuel designs. The outputs of these models are analyzed using modern data analytics and machine learning techniques to identify highly discriminating features that allow for the determination of the source reactor design, which may also inform decision making regarding the collection and measurement of nuclides of interest for monitoring and verification applications.

This paper will present an overview of the methodology that includes the use of reactor physics codes for generating fuel nuclide composition data, the data analytic approaches taken to identify nuclides and compound features of discriminatory value, and the machine learning techniques applied to the classification of source reactor designs based on the modelled nuclide dataset. The applicability of this work is demonstrated against both open source and simulated data, and shown to be of value in supporting provenance assessment for irradiated nuclear fuel.

State
Canada

Gender

Primary authors: Dr COCHRANE, Chris (Directorate of Security and Safeguards, Canadian Nuclear Safety Commission, Government of Canada); Dr EL-JABY, Ali (Directorate of Security and Safeguards, Canadian Nuclear Safety Commission, Government of Canada); Dr KHOTYLEV, Vladimir (Directorate of Assessment and Analysis, Canadian Nuclear Safety Commission, Government of Canada); UNGAR, Kurt (Health Canada); HOFFMAN, Ian (Health Canada)

Presenter: Dr EL-JABY, Ali (Directorate of Security and Safeguards, Canadian Nuclear Safety Com-
mission, Government of Canada)

**Track Classification:** MORC: Nuclear forensics
About regulatory approaches to physical protection of nuclear vessels (vessels with small modular reactors)

The Russian Federation has a unique experience in the operation of vessels powered with small modular reactors (icebreakers and lighter aboard ships). In accordance with Russian legislation, physical protection is required for the operation of such nuclear vessels. The Federal Environmental, Industrial and Nuclear Supervision Service (Rostechnadzor) is responsible for the development and support of a regulatory and legal framework for nuclear safety and security, including physical protection of nuclear vessels.

Rostechnadzor is an independent Russian state nuclear safety and security regulatory authority in the field of atomic energy use. Rostechnadzor is authorized to develop, approve and put into force federal rules and regulations in the field of atomic energy use for establishing among others requirements for the physical protection of nuclear vessels.

Currently, the following main regulatory legal acts in the field of physical protection of nuclear vessels are effective in Russia:

- "Rules for the Physical Protection of Nuclear Materials, Nuclear Installations and Storage Facilities for Nuclear Materials" (Decree of the Government of the Russian Federation);
- Requirements for the physical protection of nuclear vessels and vessels transporting nuclear materials (federal rules and regulations in the field of atomic energy use, NP-085-10).

In addition to nuclear vessels, the abovementioned regulatory documents also establish the requirements for physical protection of:

- vessels carrying out inter-facility transportation of nuclear materials;
- nuclear technology service vessels (specialized vessels for transporting, storing, performing technological operations and nuclear fuel reloading);
- floating nuclear power plants.

A physical protection system should be created at a nuclear vessel as well as at a stationary nuclear facility. Physical protection system includes a set of engineering and technical means of physical protection, physical protection personnel and organizational measures and should perform similar tasks:

- deterrence of unauthorized actions;
- timely detection of unauthorized actions;
- detention of the intruder;
- response to unauthorized actions.

But unlike a stationary nuclear facility, the provision of physical protection at nuclear vessels has its own features and differences. For example:

- priority task of the preservation of vessel vitality;
- compliance with the requirements of transport safety;
- allocation of protected areas in the limited space of the vessel;
- providing physical protection of the vessel in the pier;
- procedure for notification of unauthorized actions;
- conducting a vessel vulnerability analysis and assessment of the physical protection system effectiveness of the nuclear vessel.

These differences and features require appropriate approaches to the legal regulation of the physical protection of nuclear vessels.
The report contains the review of current state of the regulatory framework for the physical protection of nuclear vessels (vessels with small modular reactors) in the Russian Federation, the role of Rostechnadzor in the development and approval of requirements for the physical protection of such vessels, regulatory approaches to physical protection of vessels, their features and differences in comparison with stationary nuclear installations.

State

Russian Federation

Gender

Male

Primary author:  EGOROV, Alexander

Presenter:  EGOROV, Alexander

Track Classification:  PP: Nuclear security of new nuclear technologies (e.g., small modular reactors)
Review of regulations concerning physical protection of nuclear facilities in the Russian Federation

In the Russian Federation, physical protection of nuclear facilities (nuclear installations, radiation sources, storage facilities, nuclear materials and radioactive substances) is defined as an independent activity in the field of atomic energy use at the level of federal legislation. The Federal Environmental, Industrial and Nuclear Supervision Service of Russia (Rostechnadzor) is responsible for creation and support of a regulatory and legal framework for nuclear safety and security, including physical protection of nuclear facilities.

Rostechnadzor is an independent Russian state nuclear safety and security regulatory authority in the field of atomic energy use. Rostechnadzor is authorized to develop, approve and put into force federal rules and regulations in the field of atomic energy use for establishing among others requirements for the physical protection of nuclear facilities. The federal rules and regulations are legally binding on all persons carrying out activities in the field of atomic energy use and are valid throughout the Russian Federation. Rostechnadzor also develops and approves safety guides for atomic energy use, which contain recommendations on how to meet the requirements for physical protection.

When developing federal rules and regulations with requirements for physical protection, the international obligations of the Russian Federation in the field of atomic energy use and recommendations of international organizations, including recommendations of the IAEA Nuclear Security Series publications (NSS publications), are taken into account.

Currently, the following main regulatory legal acts in the field of physical protection of nuclear facilities are effective in Russia:

- “Rules for the Physical Protection of Nuclear Materials, Nuclear Installations and Storage Facilities for Nuclear Materials” (Decree of the Government of the Russian Federation);
- Requirements for the systems of physical protection of nuclear materials, nuclear facilities and storage facilities for nuclear materials (federal rules and regulations in the field of atomic energy use, NP-083-15);
- Rules for the physical protection of radiation sources, storage facilities, radioactive substances (federal rules and regulations in the field of atomic energy use, NP-034-15);
- Rules for the physical protection of radioactive substances and radiation sources during their transportation (federal rules and regulations in the field of atomic energy use, NP-073-11);
- Requirements for the physical protection of nuclear-powered vessels and vessels transporting nuclear materials (federal rules and regulations in the field of atomic energy use, NP-085-10).

The report contains:

- the review of current state of the regulatory framework for the physical protection of nuclear facilities in the Russian Federation;
- examples of the implementation of recommendations of NSS publications in federal rules and regulations in the field of atomic energy use and safety guides for atomic energy use by Rostechnadzor;
- main trends in the development of the normative regulation of physical protection in the Russian Federation and avenues for further enhancements of a regulatory framework for physical protection of Russian nuclear facilities.
State

Russian Federation

Gender

Male

Primary author:  Mr EGOROV, Alexander

Presenter:  Mr EGOROV, Alexander

Track Classification:  PP: Nuclear security of nuclear fuel cycle facilities: emerging technologies and associated challenges and complex threats
Development of Nuclear Forensics Capabilities within the Nuclear Security Regime

Nuclear forensics (NF) is internationally acknowledged as an integral part of the robust national nuclear security regime that supports law enforcement investigations of nuclear security events (NSEs). NF could deter unauthorized and malicious acts through its ability to link material to perpetrators, whereas the conclusions drawn by NF analysis about the material origin confer a valuable contribution to the prevention of future malicious acts from the same source. Moreover, by determining the origin and history of the material, NF assists the State to identify gaps and weaknesses in the applied security measures and to make informed decisions on where to strengthen its nuclear security architecture. The crucial significance of NF calls States for developing a national strategy to establish, test, enhance, and sustain their own forensics capabilities within the national nuclear security infrastructure. In this regard, the paper provides an overview on the elements and measures to be considered by the State to start developing its NF capacity and the associated actions to be taken to ensure sustaining and maintaining this capacity. The extent of the NF capabilities should commensurate with the existing and planned materials and activities in the State and it includes legal and regulatory framework incorporates NF, robust technical infrastructure, competent and sufficient human resources, and national nuclear forensics library or material information directory. Nevertheless, the national political commitment to nuclear security is vital in developing NF capabilities, as national policies that support NF are required and equally important as the NF science itself.

At the national level, NF capacity could be developed with a modest investment if the State decides to integrate the existing resources into NF capabilities. Since the State possesses a mature nuclear infrastructure, this approach would cut costs and provide new and possibly unexpected synergies between NF and other applications. The paper provides a practical insight to develop the national forensics capabilities and discusses the idea of integrating the existing national resources and infrastructure, which were created and maintained for other purposes, into NF as an effective starting point. It also portrays how the existing resources can be re-purposed for NF in line with the International Atomic Energy Agency (IAEA) recommendations and guidance and provides a roadmap for sustaining these capabilities. Moreover, the paper recommends establishing a national nuclear forensics center (NNFC), with a view to contributing to the national response plan in close cooperation with other relative authorities and institutions. Particular attention is given in the paper to the contribution of technical support organizations (TSO) and nuclear security support centers (NSSC) in maintaining and sustaining the developed NF capabilities. Recognizing the critical role of coordination and cooperation between various stakeholders in the effective management of NSE, the paper highlights the developed coordinating mechanism to ensure that the various response measures encompassing NF are taken coherently by the responsible stakeholders.

REFERENCES

3. INTERNATIONAL ATOMIC ENERGY AGENCY, Application of Nuclear Forensics in Combating Illicit Trafficking of Nuclear and Other Radioactive Material, IAEA TECDOC No. 1730, Vienna (2014).
4. ZEINAB F. AKL, "A proposed approach for developing a nuclear forensics library in Egypt", IAEA International Conference on Nuclear Security: Commitment and Actions, (Vienna, 2016)
5. Egypt, Law no. 7, The law for Organizing Nuclear and Radiation Activities, Amiri Presses, Cairo, Egypt (2010).
State
Egypt

Gender
Female

Primary author: Dr HASSAN AKL, Zeinab F. (Egyptian Nuclear and Radiological Regulatory Authority (ENRRA))

Presenter: Dr HASSAN AKL, Zeinab F. (Egyptian Nuclear and Radiological Regulatory Authority (ENRRA))

Track Classification: MORC: Nuclear forensics
Towards An Effective and Sustainable National Regulatory Oversight for Nuclear Security

Effective regulatory oversight is vital in maintaining and enhancing nuclear security at the national and global levels. Hence, a comprehensive regulatory infrastructure, comprising an efficient and independent regulatory body (RB), should be established and sustained. In addition, the RB should be provided with appropriate authority and resources concurrently with adequately qualified and competent staff to enable it to fulfill its responsibilities and functions related to nuclear security. In response to realizing the importance of developing an effective and independent nuclear regulatory system, the regulatory oversight in Egypt was anchored in the national legislation and its objectives and measures were specified as well. Over the last years, Egypt has successfully implemented measures and programs to enhance its legislative and regulatory framework related to nuclear security. In this context, a regulatory authority, known as the Egyptian Nuclear and Radiological Regulatory Authority (ENRRA) was established. ENRRA is responsible for conducting the regulatory process and activities in relation to the safety and security of nuclear and other radioactive materials, associated facilities, and associated activities. This encompasses developing regulatory requirements and guidance, issuing authorization prior to any activities entailing nuclear and other radioactive materials, and controlling the compliance of regulatory requirements and license condition through conducting inspections and taking enforcement actions in response to noncompliance. ENRRA's general regulatory policy aims at protecting people, environment, and society from the harmful effects of radiation, and it comprises aspects that are crucial for establishing and sustaining a robust regulatory architecture.

The paper provides an overview of the process of establishing and maintaining a national regulatory system for nuclear security and discusses the current regulatory functions, processes, and practices in this area. It also points out the features of the national nuclear regulatory authority and the ongoing efforts to maintain its independence, competence, continuous coordination with stakeholders, and the adequate use of advisory and support services. It also displays several activities taken by ENRRA to strengthen the supervision and control over nuclear and other radioactive materials. The main nuclear security regulatory achievements over the last years are also presented, focusing on the core functions of regulations drafting, authorization, inspection, and enforcement. Sustaining the efficiency and effectiveness of the nuclear security regulatory system throughout planning to sustain effective operations, strengthening and maintaining regulatory competence, fostering nuclear security culture, and international cooperation is also discussed. Although much had been achieved to improve the regulatory system some actions are still needed and in this context, the paper proposes some ways of further improving the effectiveness of the regulatory system for nuclear security. Moreover, it highlights some lessons learned and main challenges in regulating nuclear security.

References

State
Egypt

Gender
Female

Primary author: Dr HASSAN AKL, Zeinab F. (Egyptian Nuclear and Radiological Regulatory Authority (ENRRA))

Presenter: Dr HASSAN AKL, Zeinab F. (Egyptian Nuclear and Radiological Regulatory Authority (ENRRA))

Track Classification: CC: Implementation of national legislative and regulatory frameworks, and international instruments
Strengthening global nuclear security through counterterrorism training, equipment enhancement, and best practices

S. REPANOVICI, National Commission for Nuclear Activities Control, Safeguard, Physical Protection, Mining Section, 14 Libertatii Blvd., District 5, Bucharest, Romania
Email: sorin.repanovici@cncan.ro

Email: Jared.czap@nnsa.doe.gov

J. JONES, Independent Consultant, UK
Email: john@jejones.co.uk

Abstract
The U.S. Department of Energy/National Nuclear Security Administration (DOE/NNSA), Romanian National Commission for Nuclear Activities Control, Safeguard, Physical Protection, Mining Section, and International Atomic Energy Agency (IAEA), worked together to build a training program to strengthen the capabilities and capacities of the radiological and nuclear response teams. These enhancements were implemented by conducting training on best practices for major public event security and performing new equipment upgrades and subsequent training on the best practices to utilize these new capabilities within the overall security plan of a major public event. This culminated with the very successful use of these enhanced capabilities during the informal European Council Summit on May 9, 2019. This paper will outline the steps taken to develop this enhanced capability and will discuss future steps to ensure the responder community continues to learn and grow from experiences in nuclear security.

Introduction
Nuclear security is a nebulous and extremely complex security concern during operations like a Major Public Events (MPEs). On the one hand the likelihood of a radiological or nuclear event happening are very unlikely but the consequences can be extremely catastrophic. The consequences are not limited to loss of life or physical damage to property or infrastructure but also include the psychological effects on a population that is affected. Many security practitioners still deem many other threats that are more likely but less catastrophic risks or threats to be a higher priority on the training and resource scale. This results in challenges for the nuclear security practitioners to be able to justify training time, money and other resources to continue to evolve with the ever expanding threat. The mutual understanding of this complex threat environment allowed us to develop a training plan, equipment delivery timeline and execute these events prior to the informal European Council Summit in May 2019.

National Workshop on Nuclear Security Measures for Major Public Events
Romania hosted an expert team from the DOE/NNSA and IAEA for a training on best practices and nuclear security concepts for MPEs. The trainees came from across the security spectrum and were experts in security operations, chemical, biological, radiological and nuclear threats as well as emergency management. This training focused on the roles of the responders within the nuclear security context and how this radiological and nuclear specific security effort fits into an overall
security plan during major public events. This training also contributed to the development of the national nuclear response plan being drafted by the Romanian National Commission for Nuclear Activities Control.

**Spectral Advanced Radiological Computer System (SPARCS) equipment delivery and training**

Romania hosted an expert team from the DOE/NNSA that delivered the SPARCS equipment, conducted training on the equipment, and shared best practices for the operation and application of this detection equipment. These mobile detection systems were an enhancement to the overall security posture of the Romanian government. This training focused on the Romanian technical experts who would be managing and analyzing the complicated data that would be streaming in real time during a security operation. These experts were radiological and nuclear scientist and other technical experts that would operate and analysis the data from the SPARCS equipment.

**Informal EU Council Summit**

As stated in the IAEA Nuclear Security Fundamentals, the responsibility for nuclear security rests entirely with each State. Romania has a strong and sustainable nuclear security regime assuring the protection of persons, property, society and the environment from a criminal or unauthorized act with nuclear security implications involving nuclear and other radioactive material.

Romania hosted the Informal European Council on May 9, 2019, in Sibiu, Romania. For the first time in Romania, the National Commission for Nuclear Activities Control (CNCAN) was invited to implement Nuclear Security Measures for the Summit. As the nuclear regulatory authority, CNCAN assumed the role of coordinator of all activities related to nuclear security.

CNCAN became part of the Inter-Ministerial Committee for Security “ROMANIA – EU 2019”. CNCAN coordinated the nuclear security plan with the Protection and Guard Service (SPP), the organization with overall responsibility for coordinating security at the event. With the support of the SPP, the nuclear security plan was an integral part of the overall security plan. Between May 31 to June 2, 2019, Pope Francis will travel to Romania for an Apostolic Visit and lessoned learned during the EU Summit will be implemented during the Pope’s visit.

**Summary**

The U.S. DOE/NNSA and the Romanian National Commission for Nuclear Activities Control jointly worked together to develop a training plan that took into account the best practices from both countries experience in nuclear security as well as the training planned in conjunction with the delivery of enhanced equipment. This training plan culminated with the successful completion of the informal European Council Summit with no radiological or nuclear incidents.

**State**

United States

**Gender**

**Primary authors:** Mr CZAP, Jared (US NNSA); Mr REPANOVICI, Sorin (National Commission for Nuclear Activities Control); Mr JONES, John (Independent Consultant, UK)

**Presenter:** Mr REPANOVICI, Sorin (National Commission for Nuclear Activities Control)

**Track Classification:** MORC: Nuclear security as part of the security of major public events
Nuclear Site Security Plans based on a Claims, Argument and Evidence Approach

The Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facility (INFCIRC/225/Revision 5) Fundamental Principle E: Responsibilities of the Licence Holder: identifies that the operator should have a security plan. In the United Kingdom an approved Nuclear Site Security Plan (NSSP) is a requirement under Regulation 4 of the Nuclear Industries Security Regulations (NISR).

The National Nuclear Laboratory (NNL) is the Dutyholder for three (3) unique facilities in the United Kingdom; with nuclear assets ranging from Special Nuclear Materials through High Active Irradiated materials to nuclear materials recovery. The facilities undertake operational, and research and development activities so provide a challenging security environment.

NNL decided to take a Claims, Argument and Evidence (CAE) approach, common in the approach often taken by Safety, to meet the Fundamental Security Principles and Security Delivery Principles that are identified in the Office for Nuclear Regulations (ONR) regulatory guidance known as the “Security Delivery Principles”.

Claims, Arguments Evidence (CAE) is a logical structure in the development and presentation of an overall ‘case’, whether Safety or Security. It provides clarity of the claims that are required to be made, allows the development of the specific arguments and identifies the underpinning evidence to be shaped. CAE is an approach rather than a prescriptive format.

As the quality and extent of Security Plans increase they will often require complex, technical and multi-faceted arguments and evidence to be presented to underpin what can be essentially simple claims; “Our nuclear materials are secure from malicious threats”. Security Plans can be required to be understood, to a greater or lesser extent, by many and varied groups and stakeholders; Company Board, Facility Managers, staff, Regulators, existing and potential customers; often with varying understanding and appreciation of the technical and operational underpinning.

Those issues have the potential to drive further complexity into the security plan as all expectations and requirements are attempted to be managed resulting in the security plan being of little operational value.

As CAE is a tool which supports simplification of key elements of the security plan this paper will show how NNL have used this approach to meet multiple needs and deliver a relevant, useful and dynamic NSSPs. It will also identify how this approach can drive business improvement, regulatory confidence and understanding of risk.

NNL consider that a CAE approach to security will be relevant to operators to provide the assurances they, and their Regulator, requires whether they are working within a prescriptive or outcomes based regulatory environment.

State

United Kingdom

Gender
Primary authors:  RODGER, Robert (National Nuclear Laboratory); EDWARDS, Jeremy (National Nuclear Laboratory); Mr MOSS, Richard (National Nuclear Laboratory); Mr BROWN, Dave (National Nuclear Laboratory)

Presenter:  RODGER, Robert (National Nuclear Laboratory)

Track Classification:  PP: Application of the graded approach and defence in depth to nuclear security
Exploration on the application of Unattended and Remote Monitoring Systems at the level of government and facilities

The concept of Unattended and Remote Monitoring Systems is commonly used in the field of IAEA nuclear safeguards. Usually, those technologies such as alarm detectors, gamma or neutron detectors, video cameras and data remote transmission network are used to transmit real-time or regular measured data back to supervisory departments (e.g. IAEA). It is mainly used to supervise those nuclear materials in semi-enclosed areas or areas where staff rarely enter, which is helpful to supervisors determine whether the nuclear materials are under control. However, with the development of those technology such as “Internet +” and 5G network etc., the concept of Unattended and Remote Monitoring Systems can be further extended to expand the application of the technology in the field of nuclear security. Similar applications have been widely applied at the level of nuclear facilities. For example, for one unattended nuclear materials or radioactive source warehouses, and some automatic processing workshops of nuclear materials, etc., there is no longer a guard post at the main gate. Instead, some technologies such as door magnetic alarm and video review are adopted and managed by the remote monitoring center. However, there are many problems such as so much kinds of detection means and data transmission equipment that can be used, and many work focuses of the guard in the monitoring center, etc., which need to be systematized and integrated. This paper analyses the current situation of the development and application of Unattended and Remote Monitoring Systems, explores what problems exist in the application of those technologies in the field of nuclear security, discusses the feasibility of selective use of advanced monitoring technology at the level of government supervision for real-time or timely monitoring of key units or key parts, and puts forward countermeasures and suggestions combined with the application of new technologies.

State
Colombia

Gender
Male

Primary author: LIU, Likun (State Nuclear Secrity Technology center)
Presenter: LIU, Likun (State Nuclear Secrity Technology center)

Track Classification: CC: Advances in nuclear security research and development; international cooperation on nuclear security research
Nuclear Site Security Plans to meet Outcomes Based Regulation (or a change in Regulatory Expectations)

Within the Convention on the Physical Protection of Nuclear Material (CPPNM/A) Fundamental Principle (FP) A identifies the Responsibility of the State and FP C covers the Legislative and Regulatory Framework.

The IAEA Nuclear Security Series (NSS) document NSS13 "Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) provides that "the operator should prepare a security plan ....".

The United Kingdom competent authority ‘Office for Nuclear Regulation (ONR)’ introduced new regulatory guidance to support the Nuclear Industries Security Regulations’ This updated guidance, known as the ‘Security Assessment Principles’ to the regulatory approach further towards an Outcomes Based regulatory regime, and also to more closely align with the UKs approach to Nuclear Safety through guidance known as ‘Safety Assessments Principles’.

The ONR, to support their Inspectorate, produced a number of Technical Assessment Guides (TAGs); one for each of the thirty-eight (38) Security Delivery Principles (SyDPs).

This paper will describe the approaches and assessment methods that the National Nuclear Laboratory (NNL) used to develop their three Nuclear Site Security Plans to meet an Outcomes Based Regulatory approach. We will share the lessons we learnt from using a multi-disciplinary team approach; how we took the opportunity to go back to basics, and the processes and best relevant practice we used to deliver a challenging project.

The authors consider that the learning from experience is equally relevant to operators and technical support contractors irrespective of the type of regulatory regime they operate within.

State

United Kingdom

Gender

Primary authors: EDWARDS, jeremy (National Nuclear Laboratory); RODGER, Robert (National Nuclear Laboratory); Mr MARSH, Simon (National Nuclear Laboratory); Mr BAKER, Malcolm (Resilience Ltd and National Nuclear Laboratory)

Presenter: EDWARDS, jeremy (National Nuclear Laboratory)

Track Classification: CC: Implementation of national legislative and regulatory frameworks, and international instruments
Countering the Insider Threat

The insider threat is recognised as one of the most challenging security threats to counter in any industry or organisation, including the civil nuclear industry. All industries suffer from this threat; the financial industry with insider trading, retail with ‘shrinkage’, aviation with ‘gun running’ and ‘drugs shipping’, and there are a myriad of other examples.

It is important for the nuclear industry to address as there can be multiple consequences; unacceptable radiological consequences from sabotage, materials out of regulatory control through theft, proliferation challenges through the loss of information and technology, lost revenue through disruption of operations, and loss of public confidence and reputational damage through leaking of information.

The unique opportunities that the Insider may be given through authorised access to facilities, vital or sensitive areas or assets, and their given roles and responsibilities allowing them to widen their sphere of influence and increase the opportunity for success.

This paper looks at what an insider is, their potential motivations through consideration of the Counterproductive Workplace Behaviour Model, access, opportunity and potential consequences of a successful attack. Case studies of insider incidents from the nuclear industry, government, other industries and the military will be used to identify common criteria that can be addressed by nuclear operators. It will conclude by looking at Mitigation in Practice.

Some high profile case studies, of theft and sabotage, will be assessed to determine common fail- ures that can be addressed by operators.

The APEASE (Affordability, Practicability, Effectiveness and Cost-effectiveness, Acceptability, Side-effects/Safety, and Equity Considerations) criteria will be discussed as a business process for assessing the adequacy of proposed enhancement mitigation measures.

The paper will then look at how Dutyholders can implement Mitigation in Practice by presenting a schematic representation of protective measures (based on an approach modelled on the Cubic of Bautz) and a behavioural model known as COM-B (capability, opportunity, motivation and behaviour).

It concludes by detailing our major findings and recommendations to reduce the likelihood of insider threat.

State

United Kingdom

Gender

Primary authors:  RODGER, Robert (National Nuclear Laboratory); EDWARDS, Jeremy (National Nuclear Laboratory); Mr ROGERSON, Richard (National Nuclear Laboratory); Mr FITZPATRICK, Joshua (National Nuclear Laboratory)

Presenter:  RODGER, Robert (National Nuclear Laboratory)
Track Classification: PP: Insider threats
STUDY ON THE DEPENDENCY OF MATERIAL AMOUNTS ON BURUP IN PB-HTR BY PERTURBATION ANALYSIS

The most important issue in the material accounting of the pebble bed high temperature reactors (PB-HTRs) is to determine the amounts of the key material isotopes such as the isotopes of uranium and plutonium from the fuel burnup values obtained via calculations or measurements. The major approach to determine the production and loss of nuclear materials in the PB-HTR fuels is the burnup calculations and simulations over the actual fuel recycling process in a PB-HTR, since there is no practical isotope examination on the irradiated fuel elements of PB-HTR by now. In this work, the correlations of material amounts and the burnup values are evaluated by using the perturbation analysis on the previous results based on Monte Carlo simulations of the depletion process of the HTR-PM, the demonstration plant to be deployed in Shandong Province, China. Small perturbations are applied on the Monte Carlo simulations by adjusting the fuel recycling parameters slightly. The dependencies of material amounts of uranium and plutonium isotopes on the burnup values are concluded upon the expectation values of the stochastic distributions of the parameters mentioned above, based on the perturbed results of the Monte Carlo calculations. Furthermore, the perturbation analyses are performed on the Monte Carlo calculations for different fuel pass numbers, providing the dependencies upon the whole burnup range. The uranium isotopes present regular evolutions along with the increase of burnup values, while the plutonium isotopes present much more complicated behaviors of dependencies on burnup. The errors from the depletion calculations upon the averaged fuel composition can be avoided by using the method presented in this work.

**State**

China

**Gender**

Primary authors: Dr XIA, Bing (Institute of Nuclear and New Energy Technology, Collaborative Innovation Center of Advanced Nuclear Energy Technology, Key Laboratory of Advanced Reactor Engineering and Safety of Ministry of Education, Tsinghua University); Dr GUO, Jiong; Dr WEI, Chunlin (Institute of Nuclear and New Energy Technology, Collaborative Innovation Center of Advanced Nuclear Energy Technology, Key Laboratory of Advanced Reactor Engineering and Safety of Ministry of Education, Tsinghua University); Prof. YIN, Zaizhe (Institute of Nuclear and New Energy Technology, Collaborative Innovation Center of Advanced Nuclear Energy Technology, Key Laboratory of Advanced Reactor Engineering and Safety of Ministry of Education, Tsinghua University); Prof. TANG, Yaping (Institute of Nuclear and New Energy Technology, Collaborative Innovation Center of Advanced Nuclear Energy Technology, Key Laboratory of Advanced Reactor Engineering and Safety of Ministry of Education, Tsinghua University)
Presenter: Dr XIA, Bing (Institute of Nuclear and New Energy Technology, Collaborative Innovation Center of Advanced Nuclear Energy Technology, Key Laboratory of Advanced Reactor Engineering and Safety of Ministry of Education, Tsinghua University)

Track Classification: PP: Nuclear material accounting and control
Modelling and Simulation to inform decision making on Physical Protection Solution and Land Management

Monday, 10 February 2020 15:30 (15 minutes)

Modelling and Simulation (M&S) in nuclear safety applications is commonplace, for example to underpin and inform criticality, dose and shielding assessment. However, the adoption of modelling and simulation for nuclear security has not seen the uptake that many anticipated. This is despite significant advances being made in the capability of equivalent tools for nuclear security, coupled with the potentially significant cost savings that could be achieved. Further, despite workshops/initiatives by organisations such as the Institute of Nuclear Materials Management (INMM), and development of best practice guides by the World Institute of Nuclear Security, evidence of M&S tools being used to inform decisions in the nuclear sector are not well publicised.

This paper intends to present the results of work undertaken jointly by the National Nuclear Laboratory on behalf of Magnox Limited and the Nuclear Decommissioning Authority (NDA) to provide evidence upon which future land use and security infrastructure decisions can be made. Magnox Limited are responsible for the management and decommissioning of the early UK Magnox reactor fleet, and a number of early UK nuclear programme research and development sites. These sites are owned by the Nuclear Decommissioning Authority, who sponsored this application of modelling and simulation to this project.

The ARES Security Corporation. AVERT product was utilised for conducting a programme of work to assess potential future changes to a site perimeter, and also its policing and guarding arrangements. The outcome of this work is to be used to inform future investment decisions on infrastructure modifications with the intention of being able to reduce the overall footprint of the site and release land back for redevelopment. Coupled with this will be the necessary changes to the policing and guarding posture commensurate with providing the guarding and response for a smaller site.

The site has been re-created in 3-dimensions using existing engineering models built in CAD, along with options for future potential layouts/configurations. The work utilises the UK Design Basis Threat known as the Nuclear Industries Malicious Capabilities and Planning Assumptions (NIMCA) document to derive the postulated scenarios and adversarial capabilities that the site is required to mitigate against. These have been integrated into modelled scenarios to determine overall security system effectiveness as a measure for comparison between the options. The scenarios that are being assessed are also aligned to those used in the Vital Area Identification process.

Analysis of the comprehensive model output files enables interrogation of key scenarios and key events. This provides an unrivalled insight to the progression of an adversarial attack, their interaction with the integrated Physical Protection System (PPS), and determine the effectiveness of the various layers and components.

The paper will present comparative results arising from the work and their use in aiding decision making on future land-use, and the associated policing and guarding arrangements. Key challenges and benefits associated with the use of modelling and simulation will also be presented to further inform the debate and development of these innovative approaches.

Acknowledgements:
Our appreciation and thanks are extended to the Nuclear Decommissioning Authority for their sponsorship of this work, and to Magnox Limited for their engagement and participation in the successful delivery of the project.
State

United Kingdom

Gender

**Primary authors:**  RODGER, Robert (National Nuclear Laboratory); EDWARDS, jeremy (National Nuclear Laboratory); Mr BURKMAR, Richard (Magnox Ltd); Mr UNDERWOOD, Nick (National Nuclear Laboratory); Mr TONKS, Paul (Nuclear Decommissioning Authority); Mr WILLIAMS, Chris (Nuclear Decommissioning Authority)

**Presenters:**  RODGER, Robert (National Nuclear Laboratory); EDWARDS, jeremy (National Nuclear Laboratory)

**Session Classification:**  Physical protection systems: evaluation and assessment

**Track Classification:**  PP: Physical protection systems: evaluation and assessment
Strengthening the security of nuclear and radioactive Material during transport

Despite the benefit provided by nuclear and other radioactive material to human beings in different activities, they also have the ability to cause a great damage if are poorly secured. For this reason securing Nuclear and other Radioactive Material during transport is considered as big must as necessary concerns to state either at the international or national level.

In addition, the threat has grown very faster in the latest decades, due to the existence of the terrorist groups that are seeking the Nuclear or other Radioactive Material to be used in their attacks likewise, the consciousness that threaten the Nuclear security has grown too.

In fact, the Transport security of nuclear and other radioactive material faces many challenges among them, that the process is considered as the most vulnerable activity in the life cycle of the items, which make it vulnerable to the theft and sabotage because it takes place outside of secured facilities and near of public. Also the transport involves several entities, moreover the responsibility of securing them might have been transferred from the entity to another ones several times which means that the Nature of the threat might also change.

Further to the fact given above, Inneffective national regulations and regulatory body monitoring Poor design of nuclear security functions and physical protection systems, lack of the knowledge about the importance of nuclear security culture and communication between the entities Involved in the operation could lead to the loss of control to manage the transport security.

To respond on how to minimize the risk, several international instruments have been developed by the International Atomic Energy Agency to manage the Nuclear Security such as Regulations, Conventions, Fundamentals and Recommendations to assist the member state for enhancing the Nuclear Security and raising awarness about the importance to secure the Nuclear and other radioactive material during national and international transport.

Among of them, The Convention on the Physical Protection of Nuclear Material (CPPNM) and its Amendement, which is the only legally binding that should be ratified by the state in order to be integrated in the development of state’s National Regulation on Nuclear Security.

Neither, The code of conduct on the safety and security of Radioactive Sources as an international instruments, the Security in the Transport of Radioactive material (IAEA Nuclear Security Series No. 9) which provides the necessary obligations to maintain the security of transport and address the role and responsibilities to the each entities involved in the operation, similary the IAEA Nuclear Security Series No. 26-G Implementing Guide Security of Nuclear Material in Transport which provides a deep requirements from addressing roles and responsibilities, designing and maintaining a physical protection regime either designing the physical protection system to the requirements to recover missing nuclear material during transport.

Securing Nuclear and radioactive materials during transport remains and requires the designation of an intelligent national authority regulatory body and the development of legislative and regulatory framework to keep nuclear and radioactive material more secured during transport to detect, deter and delay any unauthorized removal of Nuclear and other radioactive material.

Physical Protection is a matter of the international community, However to strenght a higher level of transport security, the state should develop an effective physical protection regime during transport according to the categorization of Nuclear and radioactive materials and the risk that could cause taking into account the graded approach, defence in depth, the quantity of nuclear or radioactive material shipped and their attractiveness to protect people, property and the environment from malicious acts which is the main goals of the nuclear security.
Physical protection measures (Detection, Delay and response) have to be designed and evaluated before the operation to prevent the adversary tasks either the nuclear security plan. Furthermore, in this paper focused on discuss the role and the responsibility of the state to develop, maintain and design an effective nuclear security and the physical protection regimes based on the graded approach and defence in depth to strengthen the security of transport, that are the eligibility fundamental principals for sustaining an effective nuclear security measures to enhance the security of transport of nuclear and other radioactive material, keeping in the mind to enhancing the nuclear security culture among stockholder’s (consignee and the consignor) to secure the materials, also we are going to propose the physical protection systems designs and the nuclear security functions measures according to the category on nuclear and other radioactive material to strengthen their security during transport taking into consideration the level of each category and the design basis threat, graded approach and defence in depth that are the keys of an effective nuclear security measures that should be taken in shipment also we are going to highlight about the importance of the communication between response forces during the transport.

State
Morocco

Gender
Female

Primary author: TOUARSI, AMAL (PHD STUDENT ON TRANSPORT SECURITY OF NUCLEAR AND RADIOLOGICAL MATERIAL UNIVERSITY OF IBN TOFQL KENITRQ MOROCCO)

Co-author: KHARCHAF, Amina (Professor at Ibn Tofail University, physics Department, Doctor on reactor Physics)

Presenter: TOUARSI, AMAL (PHD STUDENT ON TRANSPORT SECURITY OF NUCLEAR AND RADIOLOGICAL MATERIAL UNIVERSITY OF IBN TOFQL KENITRQ MOROCCO)

Track Classification: PP: Transport of nuclear and other radioactive material: practices, challenges and regulatory issues
INTEGRATING CYBER AND PHYSICAL SECURITY: ENHANCING SECURITY CULTURE FOR NUCLEAR POWER PLANTS (NPP) – A PROSPECTIVE METHODOLOGY FOR TURKEY

Nuclear Power Plants (NPP) are globally most protected critical infrastructure in the sector. The Fukushima accident was a wake-up call for reminding the international community about the possible outcomes. Today, methods to protect critical infrastructures in the security sector are rapidly transforming due to the rapid changes in cyber, physical and hybrid threats which are exponentially increasing because of the global political and economic shifts. In addition to the physical security threats, cyberspace is becoming a major concern for the NPP operators and governments. The continuous integration of the cyber and physical domains in NPPs is not only representing risks, but it also presents various opportunities such as the reduced costs and higher efficiency. However, the rapidly growing digitization and over reliance on the computer-based systems in the operation returned nuclear material accountancy and the perimeter security systems of the NPPs into targets for cyber/physical attacks.

On the other hand, physical and cyber security were largely seen as two distinct domains and cultures in the past, today, in contrast, the equipment also used in the physical protection in critical infrastructures (CI) such as CCTV cameras, sensors, any physical access regulating systems also rely on the computing systems which are mostly not segmented and connected to a network. This functional integration also makes them vulnerable to cyber attacks particularly those which could create a devastating impact in the physical and kinetic world. Even though the problems and threats identical, the staff in the cyber and physical security disciples are generally approaching same problems from different perspectives and they have limited communication among themselves.

Both parties have their own security cultures due to their backgrounds and approaches. When the recent threat range and implementation of the hybridity is considered, to build an integrated security culture is a necessity. In that respect, the integration of cyber-physical security cultures seems as a must in order to timely detect the security incidents as well as to respond them in real time in order to enhance resiliency. At that point, it should be underlined that simplistic security management merging cannot help to solve the problems. Integrated security culture requires an effective cooperation which also should include a proper information sharing practice, collaborative planning methods, strategic communication, launching new training platforms, implementing shared risk management practices and much more where the different security experts of the both disciplines could combine resources to achieve to protection goals.

From the Turkish perspective, Turkey is a relatively newcomer to NPP environment with respect to diversifying its energy supply sources to meet its constantly increasing energy demand. In that respect, even though currently there is no NPP in operation in Turkey, it is planned that Turkey will install the first nuclear power plant that started to be constructed and will be operated in Akkuyu - Mersin Province with the ROSATOM. However, particularly from a cyber security perspective, it could be said that currently Turkey has limited experience as a regulator for NPPs. Even though, Turkey has intention to implement crucial and effective policies in the cyber security field like launching a national cyber security strategy as well as the creation of Cyber Emergency Response Team (CERT), it is possible to claim that the increasing cyber-physical security challenges, as well at rapidly transforming threat landscape requires a more sophisticated knowledge and specialized know-how particularly for securing NPPs including an integrated cyber-physical security approach. More importantly, this approach and integration must be embedded in an effective security culture.

In that respect, this research paper merely aims to focus on the following research questions: How
the cyber-physical security integration could be performed for an integrated security culture for Turkish nuclear energy agenda? Since human factor is vital for an effective nuclear security, how the skilled human capital could be trained to achieve this goal? What should be the role of national regulator agency and the operator in this respect?

State

Turkey

Gender

Primary authors: Prof. BIÇAKÇI, Ahmet Salih (Associate Professor, Kadir Has University, International Relations Department; Center for Cybersecurity & Critical Infrastructure Protection); Mrs GUCÜYENER EVREN, Ayhan (PhD Student/Project Specialist, Kadir Has University, Center for Cybersecurity & Critical Infrastructure Protection)

Presenter: Prof. BIÇAKÇI, Ahmet Salih (Associate Professor, Kadir Has University, International Relations Department; Center for Cybersecurity & Critical Infrastructure Protection)

Track Classification: CC: Nuclear security culture in practice with a focus on sustainability
Delivering Security by Design on a Multi-faceted Project

On too many occasions the first input that the security team have to influence the security arrangements at a facility is after the design is agreed and the work is underway; or building use is modified; or the threat landscape changes. Thus, the security arrangements must be retrofitted within restricted footprints, and often within operational and Radioactive Controlled Areas (RCAs), resulting in increased capital (and operational) cost, reduced capability and compromise between safety, operations and security. The economic pressures on nuclear being able to compete with other forms of technology are driving various initiatives such as the Nuclear Energy Institute ‘Nuclear Promise’ in the US, and the UK Nuclear Sector Deal. The latter aspires to reduce the costs of new nuclear build by 30% by 2030, and 20% reduction in decommissioning projects.

Security by design is referenced within INFCIRC 225, Rev 5, and increasingly is the recognition that inherent safety and security arrangements are cheaper and more effective if incorporated prior to construction or operation. The UK’s National Nuclear Laboratory is currently supporting a concept design project for a facility which will operate for many decades. An integrated project team, led by the Safety, Security and Safeguards team have an active role in influencing security from the outset, based on UK guidance provided by the Centre for the Protection of National Infrastructure’s in their Operational Requirements process. Working with the Engineering Design team has already provided great benefit and the opportunity to realise ‘security by design’. This paper discusses the experiences thus far.

Insight to the application of a systematic approach is presented. Engineering and design projects should lend themselves to integration of security requirements, typically being based upon well defined, phased design stages to allow for iterative development of the design as requirements become better defined, risks and uncertainties addressed, and importantly the close marriage between the evolution of the design in tandem with the safety case. UK nuclear regulation places key milestones and regulatory decision points during the evolution of a project. This approach is based upon historic learning and adoption of best practice.

So why then has security not been a core element of engineering and design projects? In part this is due to culture – historically one where security was the ‘dark art’, perceived to be ‘done to a project’ rather than a key component to successful delivery. Perversely, the security that used to shroud security requirements and security specialists is precisely the reason why security was not integrated into design process. The changing threat landscape, global initiatives to combat nuclear terrorism and malicious use of radiological and nuclear materials, enhanced transparency and guidance from bodies such as the IAEA, development of best practice from Non-Governmental Organisations such as the World Institute of Nuclear Security (WINS), and other drivers have all assisted change. In the UK, the integration of the safety and security nuclear regulators to form the Office for Nuclear Regulation (ONR) and a move away from a more prescriptive, to an outcome based regulatory approach placing the onus more clearly on the dutyholder, or operator, have increased the need for a change in approach.

The project team have worked on the development of a Systematic Approach to be adopted that addresses Information, Assessment, Decisions and Processes. It has integrated Best Relevant Practice (BRP) and Learning from Experience (LFE); coupled with a keen focus on the inclusive, interaction with stakeholders and multi-disciplinary capabilities. Absolutely key to which has been the integration of safety, engineering and security; along with operational personnel, and guard force representation.

Presented will be an outline of the approach, the experiences and learning developed throughout
the Concept Design phase and the further development in Preliminary Design. The key benefits will be highlighted, along with those key areas of learning that can be adopted by others.

**State**

United Kingdom

**Gender**

**Primary authors:** RODGER, Robert (National Nuclear Laboratory); EDWARDS, jeremy (National Nuclear Laboratory); Mr BAKER, Malcolm (Resilience Ltd and National Nuclear Laboratory); Mr MARSH, Simon (National Nuclear Laboratory); Mr BONE, Jason (Sellafield Limited)

**Presenters:** RODGER, Robert (National Nuclear Laboratory); EDWARDS, jeremy (National Nuclear Laboratory)

**Track Classification:** PP: Security by design, including in newcomer countries
The Integration of Safety and Security Teams to Enhance Value to Customers and Projects

At the 34th G8 Summit in Japan in 2008 the assembled leaders acknowledged the role of nuclear power in reducing CO2 emissions. Part of the final communique stated their commitment to the highest possible standards on “nuclear non-proliferation, safeguards, safety and security”. They recognised that synergies exist between the Triple Ss, (nuclear safety, nuclear security, and nuclear safeguards) and considered it was important that the separate disciplines are integrated, and that the Triple S infrastructure is strengthened through international cooperation and assistance.

The National Nuclear Laboratory (NNL) brought together their Safety and Security assessment teams and their Safeguards Programme Management into a single management chain in 2016. This paper will describe how the safety and security assessment teams (2S) have been successfully working together as a multi-disciplinary team to provide enhanced value to internal and external customers.

The paper considers which approaches, methods and processes can contribute most to improving the integration of safety and security.

It acknowledges the individual aims:
Safety is aimed at protecting workers and the public from the harmful effects of radiation (or chemicals or other hazards);
Security is aimed at preventing malicious acts that might harm a nuclear facility (sabotage) or result in the loss (theft) of nuclear materials; and
And how they share the same overall objectives of protecting the public and the environment from the hazards associated with the nuclear industry.

The principles to achieve protection; multiple barriers, defence in depth, decision analysis and consequence assessment; are discussed. The regulatory regimes for safety and security use, in the main, the same processes; assessment, permissioning, inspection, enforcement and influence.

NNL’s Learning from Experience through close and integrated working will be shared. Our experience includes the removal of ‘silo working’, the development of collaborative relationships, and the cross-fertilisation of knowledge between disciplines. Some of the existing challenges to closer co-operation and alignment will also be explored and potential mitigation methods considered.

Specialists in Safety and Security need to become more aware of the priorities, approaches, methods and drivers that the other specialists use in delivering their objectives to develop and promote an integrated approach. Early interaction reduces the potential for conflict, and allows identification on where negative interactions may occur. Thus potentially expensive rework or compromises are removed.

It is our experience that integration of 2S is more likely to be achieved and be effective in the early design and construction phases of a project, with the positive effects being an influence through operations. Thus ongoing costs are optimised.

Integration of Triple S is a positive management approach to use throughout a project or a facility’s lifetime as it allows the interactions and boundaries to be more clearly understood so that a right first time outcome is achieved and potential conflicts are removed. This also leads to more streamlined operations and subsequent cost savings. It can also lead to reduced radiological doses and more effective cross-specialism communication and interactions.

2S is leading to increasing professionalism as methods and techniques used by one group of specialists are adapted and used by others through sharing of knowledge and learning from experience.

From a security perspective replacing the ‘Need to Know’ with the ‘Need to Share’ has eradicated
the ‘Dark Art of Security’ and improved organisational buy-in to the security delivery objectives. We are finding that interaction with the other specialist can lead you to reconsider how you do your work and what information is important such that nuclear safety and nuclear security are more effectively integrated.

State

United Kingdom

Gender

**Primary authors:** Mr MARSH, Simon (National Nuclear Laboratory); RODGER, Robert (National Nuclear Laboratory); EDWARDS, jeremy (National Nuclear Laboratory); Dr BENNETT, Simon (National Nuclear Laboratory)

**Presenter:** Mr MARSH, Simon (National Nuclear Laboratory)

**Track Classification:** CC: Nuclear safety and security interfaces
Investigating The Role of Swipe Samples in Strengthening Nuclear Forensics and Sustaining Nuclear Security

Nuclear forensics is an effective technical tool for investigating nuclear materials, its properties, and its history. The importance of nuclear forensics has emerged as a result of the spread and growing phenomenon of terrorism. To get rid of this phenomenon, the international community supports any effort to strengthen and maintain a robust nuclear security system. The application of environmental monitoring as a recently developed tool to identify processes related to the nuclear fuel cycle has been suggested by international safeguards.

The work describes the robust nuclear security system in the point of view of implementing a national framework for nuclear forensic capability and technical tools and instruments required for nuclear forensics. Techniques such as gamma spectrometry, radiochemical separation, inductively coupled plasma using optical emission spectrometer or mass spectrometer are powerful for revealing information related to nuclear materials in any form. Nuclear materials can be in a form of traces such type of samples to be characterized a swipe sample should be taken and introduced to one of the above techniques.

The paper focuses on assaying five environmental samples from nuclear facilities to test whether it contains nuclear material or not. The Scanning Electron Microscope (SEM) and Energy Dispersive X-ray (EDX) tools are used to localize particles, counting the targeted particles and x-ray is used to know the concentration of each element. The SEM used in this study was a JEOL JSM-6510LV-Japan with a resolution of 1pA0 to 1μA0. The five environmental samples were measured at different conditions of magnifications and working voltages. Two types of EDX analysis are used the area analysis and the spot analysis. The spot size is adjusted at the optimum value (50) also the working distance (9:11).

Finally, nuclear forensics has a vital role within a national nuclear security infrastructure. National policymakers, competent authorities, law enforcement, and technical personnel should be aware of this role. Environmental samples analysis need more sophisticated techniques like ICP-MS, alpha spectrometer to reveal its secrets beside SEM coupled with EDX. SEM and EDX are robust techniques to localize microparticles, counting the number of uranium or thorium particles and determining the concentration of each particle within the sample. The use of spot analysis in SEM images gives fast and accurate results about the nuclear materials within samples.

State

Egypt

Gender

Male

Primary author:  Dr SHABAN , Sameh

Co-authors:  Prof. ZIDAN , Walid;  Prof. ELSHEREAFY, El sayed;  Dr KAMEL , Zinab
Presenter: Dr SHABAN, Sameh

Track Classification: MORC: Nuclear forensics
Nuclear security inspections; the Hungarian way

Hungary is rich in radioactivity related activities as there is a nuclear power plant operating with four reactors, a spent fuel interim storage facility, a research and a training reactors, and two radioactive disposal facilities next to the around four hundred radioactive source users. Because of the amount of possible inspection locations the Hungarian Atomic Energy Authority (HAEA), having all the regulatory rights in all nuclear related fields, had to introduce a multilevel nuclear security inspection system.

The Hungarian regulation states, that the HAEA has the duty of licensing, inspections and enforcement in all radioactivity related activities. In nuclear security the Hungarian National Police has a co-authority right, which means that for an approval during licensing their support is mandatory. The Police also has the right to carry out inspections with or without the HAEA.

Inside the HAEA the Section of Nuclear Security and Safeguards (SNSS) handles all the security licensing tasks and also carries out performance-based inspections in the facility level licensees. These inspections could be announced and unannounced, and usually have a three pillar structure: every time something is tested in relation with the detection or delay systems, with the response forces and also there is always a documentation verification. All the inspectors of this section have university degrees in energy engineering or security and continuously trained both on national and international courses.

Next to the dedicated security inspections there are around two hundred complex inspections where both radiation safety, material inventory and security are inspected. These are carried out by regional inspectors, members of the Section of Integrated Inspections (SII), whose main task is to carry out all the inspection related activities of all the licensees in two or three counties. Many of these regional inspectors has a background of radiation protection and were later trained in the other two fields. They are fully equipped to carry out the tasks with having their own radiation detectors and all the necessary logistical tools. To ensure that all the necessary fields are inspected they use a special, user friendly, check box type inspection format. Beyond being trained in the regulatory processes they are also capable to work with the mobile expert support teams in case of a lost or found radioactive source.

There is a regulated interaction between the two sections: the security license application containing the Physical Protection Plan, is evaluated and approved by the SNSS, and if it is not a facility level sites, the inspectors of the IIS will go and make an inspection there in accordance with their annual inspection plan. If any of the sections finds something different from the regulation or the approved Physical Protection Plans, their task is to carry out an enforcement action. It the regional inspectors discover a deviation in a high category radioactive source user, than the inspectors of SNSS can have a dedicated security inspection there with the participation of members of the National Police.

The future challenges and plans of the HAEA in nuclear security inspections, is to increase its personnel, maintain the efficiency of all the inspection individually, to increase the level of training for regional inspectors and to raise the number of dedicated inspection both on facility level and on the high category radioactive users’ sites. With the help of these developments the HAEA can efficiently ensure and if necessary enforce the compliance with the regulations.

State

Hungary
Gender

**Primary authors:** Mr VIPLAK, Armand Máté; Ms HÓDOSI, Viktória
**Presenter:** Mr VIPLAK, Armand Máté

**Track Classification:** CC: National nuclear security inspections: training of inspectors, development of procedures and managing findings
International Co… / Report of Contributions Integrated Response Training Foc…

Contribution ID: 349  Type: Paper

Integrated Response Training Focused On Soft Targets Housing Radiological Sources-A Flexible Approach

It is a widely accepted premise that terrorists seek to acquire radioactive materials with the objective of causing both harm and disruption on a major scale. The United States Depart of Energy’s Office of Radiological Security (ORS) has taken a multi-tiered approach to securing soft targets (e.g., universities and hospitals), which house radioactive materials for research and medical use. The first prong was that various security upgrades were provided by ORS to these (soft) sites in order to increase the security posture surrounding these materials. Though an important step, ORS recognized that detection and delay measures at a site are meaningless if there is not a timely and effective response from the local law enforcement agency.

Thus the second tier was introduced by ORS in the form of the Response Training Academy located at the Y-12 National Security Complex in Oak Ridge, Tennessee which provides multiple training resources to engage sites coupled with their local law enforcement so that the law enforcement is aware and prepared to respond to a site’s criminal/terrorist event involving radioactive materials.

Alarm Response Training (ART) is the primary training program provided by the ORS and is specifically tailored to the responsible on-site and their local responders who support the protection of sites that have radiological and nuclear (R/N) materials. This training program directly supports the ORS protection strategy through the promotion of a timely, well prepared, and coordinated response that has the capability to prevent the theft of nuclear and radiological materials. The ART course combines classroom instruction, tabletop exercises, and hands-on training for on-site security, law enforcement, radiation safety officers, safety personnel, and other responders.

ART has proven to be an extremely effective program when presented in a domestic environment. Each soft site is supported by a local jurisdictional police department. Though there are over ten thousand police departments in the United States, each one is task organized in a similar fashion with comparable tactics, techniques and procedures. The “United States model of policing” has not proven to be the case with partner nations. Something other than a “one size fits all” approach to radiological source security needs to be examined.

Experience with numerous partner nations attending ART has shown that each partner nation has its own unique approach to response as their policing methodologies are varied as is the equipment carried by their local police (e.g. armed, unarmed). A common theme heard from our partner countries was that the ART training concepts (particularly the academic portion) were absolutely valid with respect to their individual countries, though their response protocols varies from the US model (as demonstrated during the ). As response procedures are varied between partner countries, the ART training approach must also be flexible to the individual partner country’s needs.

ART course international approach regarding content flexibility begins with a needs assessment developed during discussions with the partner country. These discussions will outline partner country’s response force procedures and protocols, along with laws specific to sites containing radiological sources located in the partner country.

In this manner, the development of a proven radiological response program that integrates all aspects of radiological response can be customized to each individual partner country’s needs. The partner countries ability to conduct a timely and effectively response by local law enforcement (and others) will be greatly enhanced in stopping a criminal or terrorist event involving radioactive materials.

The Office of Radiological Security provides tools to build and reinforce ties between sites and their local law enforcement agency so that responders are prepared to thwart the most determined
of adversaries from obtaining radioactive materials. Alarm Response Training’s proven training methods along with its flexibility to adapt partner countries response protocols will be presented.

**State**
United States

**Gender**
Male

**Primary author:** Mr ROMANO, Daniel (US DOE)

**Presenter:** Mr ROMANO, Daniel (US DOE)

**Track Classification:** CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
Nuclear Security of Research Reactors: The Effective use of INSSP process and Building a Robust Regime

The objective of a State's nuclear security regime is to protect persons, property, society, and the environment from the harmful consequences of a nuclear security event. To accomplish this aim, States exert enough efforts in establishing, implementing, maintaining and sustaining an effective and appropriate nuclear security regime to prevent, detect and respond to such nuclear security events.

Nuclear and radioactive material could be misused to be a part of malicious acts and this is regarded as a serious threat to international security and peace. It is well known that the state has many responsibilities to construct nuclear security and that appropriate and effective national systems for nuclear security are vital in facilitating the uses of nuclear energy peacefully and enhancing global efforts to combat nuclear terrorism. The IAEA-developed Integrated Nuclear Security Support Plan (INSSP) provides States, upon request, with a systematic and comprehensive framework for reviewing their nuclear security regimes and identifying areas where they need to be strengthened. The Plans also highlight any support required to help in developing an effective and sustainable nuclear security regime. Because of its flexible and tailored approach, the INSSP can be useful for all States regardless of their nuclear security regime status.

The paper discusses the importance of nuclear security system within a research reactor facility and it highlights the most important elements of establishing, maintaining and sustaining a robust nuclear security regime. It also focuses on the INSSP purpose, INSSP development process, organizations usually involved in implementing activities in INSSPs and INSSP Nuclear Security Activity Categories. Finally, the paper overviews the assistance of the IAEA to states Integrated Nuclear Security Support Plan and the effect of this assistance to enhance and maintain its national nuclear security regime.

Eventually, building an effective and efficient nuclear security regime is essential for any state. Such a system to be robust should apply fundamental issues that are mentioned in IAEA publications. IAEA helps states in enhancing and developing its nuclear security regime through IPPAS and INSSP. INSSP aims at developing legislative and Regulatory Framework, prevention, detection, response and sustainability (Human Resource Development).

State
Egypt

Gender
Male

Primary author: SHABAN, Sameh (lecturer)
Co-authors: HAZZAA, Mohamed Helmy Mohamed (Egypt); Dr EL-TAYEBANY, Rasha (Egyptian Nuclear and Radiological Regulatory Authority (ENRRA).
Presenter: SHABAN, Sameh (lecturer)
**Track Classification:** CC: Identification of national needs through the development of an Integrated Nuclear Security Support Plan
Cyber incidents are the norm in every industry, and the nuclear industry is no different. However, the effects of an incident are different in the nuclear sector, where consequences are heightened by fears of radiation releases and material diversion. In an era of fake news that often spreads on social networks quicker than accurate official reports, incident planning needs to be prioritized and given a fresh look.

That was just one finding from a workshop on nuclear cyber risks held in Vienna, Austria, in late 2018. The Fissile Materials Working Group (FMWG) - a coalition of 80 organizations from around the world working to keep the world safe from nuclear terrorism - in collaboration with the Stimson Center brought together cybersecurity experts and stakeholders to consider cyber risks in the civil nuclear industry and how to address them. The workshop report, Nuclear Cybersecurity: Risks and Remedies, details 10 findings.

Since the time of that report, FMWG and Stimson have been working with expert stakeholders to further assess those risks, to consider new emerging risks, and to prioritize actions needed to better manage them.

In the cyber incident management example, it was found that more scenario-driven exercises are needed, as well as joint development of possible approaches to misinformation and the creation of an “accurate news” repository. With artificial intelligence (AI) now assisting the development of “deepfakes,” disinformation has become an even greater challenge to officials looking to convey appropriate emergency information after a nuclear/radiological event. Efforts to develop good approaches to this challenge should be coordinated with IAEA emergency response work and could be exercised through both new and existing forums, such as the Global Initiative to Counter Nuclear Terrorism (GICNT) exercises.

The issue of secrecy in security also presents a sector challenge, with management of nuclear security being more close hold than in some other sectors. One way to address the requirement for secrecy is the establishment of an anonymized database comprising lessons learnt regarding security incidents, be they accidental/intentional or cyber/physical/combined. An “operator database” resource should be developed from opensource reporting and voluntary sharing and may include safety incidents with cyber-components. The database should also include incidents on industrial control systems from other industries that could affect the nuclear sector.

New approaches are needed to reduce risks. Some, for example, have suggested nontargeting of nuclear power plants including via cyber intrusions. But to enforce agreement on this, cyber attribution would be needed. This paper will detail some new work being done in the private sector and civil society to help with attribution.

The paper will also consider new technologies. Unmanned aerial vehicles and wearable digital devices already threaten information security and potentially nuclear facility operations. Some even newer technologies can also be a help to security as well as a threat. For example, robotics and remotely-operated weapon systems all can assist in making security more cost efficient and could be an effective attack deterrent. However, these also present additional attack surfaces for cyber intrusion. An understudied factor is any catastrophic incidents occurring from the misuses of new technologies and machine intelligence, which are so unknown, will almost certainly be unpreventable and beyond the design basis threat of any nuclear facility.

What is the nuclear industry to do? And what can governments do to help address these risks?
The original work of the first FMWG-Stimson workshop – an assessment of nuclear cyber risks and recommendations for addressing those risks – is in the process of being analyzed with input from dozens of expert stakeholders. This paper presents an updated analysis that considers even newer risks, recounts some of the work being done to address nuclear cyber risks and presents recommendations for actions to be undertaken to manage these risks.

State
United States

Gender
Female

Primary authors: Ms DECKER, Debra (Stimson Center); Ms RAUHUT, Kathryn (Stimson Center); Mr FABRO, Mark (Lofty Perch)

Presenters: Ms DECKER, Debra (Stimson Center); Ms RAUHUT, Kathryn (Stimson Center); Mr FABRO, Mark (Lofty Perch)

Session Classification: Risks and benefits to nuclear security from innovations in other fields, including artificial intelligence and big data

Track Classification: CC: Information and computer security considerations for nuclear security
Nuclear Facility Low Altitude Threat and Defense Technology

Monday, 10 February 2020 17:45 (15 minutes)

With the rapid development of high and new technology, Low-altitude, Slow-speed and Small-sized Aircraft (hereinafter to be referred as LSSA), represented by UAV, paraglider, hot air balloon and other light aircraft, are becoming more and more widely used. However, due to the fact that the corresponding regulations and technical measures still lag behind, the rapid development of LSSA brings lots of serious new challenges to nuclear security issues.

There are lots of concerns regarding the boundary of a facility’s anti-aircraft capacity. So the first chapter of this paper discusses the potential consequence of different type of malicious acts with LSSA, such as technical investigation, illegal transportation, direct sabotage, public-opinion influence, uncontrolled falling, electromagnetic interference and intrusion assistance. This chapter also analyses the low-altitude threat situations based on the research above and sorts out the threat forms and protection strategies that different nuclear facilities should focus on accordingly.

The second chapter aims at introducing the regulatory system and legislation actions of Chinese central government concerning the “LSSA threat” of most valuable facilities, as well as the problems and solutions of corresponding law enforcement practices conducted by some local governments. In addition, the technical criterion framework under the exiting legal system for low-altitude defense of nuclear facilities compiled by the State Nuclear Security Technology Center (SNSTC) is also presented in this part of the paper.

In the third chapter, I elaborates the advantages and disadvantages of some available detecting technology, including radar, intelligent video, frequency spectrum surveillance, sonar, and TDOA. Sequentially, this chapter analyzes the pros and cons of available response(suppression) technology like laser, micro-wave, net capture, protocol decoding, navigation trick, and frequency disturbance. According to the analysis of various technical paths, this chapter puts forward a systematized solution that consists suitable detect and response technical measures. In addition, this chapter provides some details regarding how State Nuclear Security Technology Center (SNSTC) inspects and verifies these technical measures.

At present, there are some nuclear power plants in China that have already enhanced their capacity to prevent and mitigate low altitude threat. In fourth chapter, the author takes NPPs in Yangjiang, Ningde and Changjiang as three examples so as to introduce different experience and feedback in different stages, including operation, construction and preparation of LSSA defense practice. This chapter introduces a Symposium on Nuclear Facility Low-altitude Threat and Mitigation, which was jointly held by Chinese Nuclear Society, State Nuclear Security Technology Center(SNSTC), undertook by China Nuclear Power Engineering Co in 2019. Some consensus and achievements of the symposium are demonstrated in this chapter.

In last chapter, a conclusion as well as some expectations and proposals are put forward.
Primary author:  Mr ZHAO, Zeyu (State Nuclear Security Technology Center)

Co-author:  Mrs GUO, Xuan (China Nuclear Power Engineering Co)

Presenters:  Mr ZHAO, Zeyu (State Nuclear Security Technology Center); Mrs GUO, Xuan (China Nuclear Power Engineering Co)

Session Classification:  Risks and benefits to nuclear security from innovations in other fields, including artificial intelligence and big data

Track Classification:  CC: Risks and benefits to nuclear security from innovations in other fields, including artificial intelligence and big data
Gender Stereotypes. Woman in Nuclear Security

This article is not about violation of rights of woman or man. This article is about deep understanding, that differences are combine. There is no need to underline, that traditionally security area is a “man area”, even nuclear science was “man area” not so far ago. Nevertheless, things are changing and we need to consider this. Worlds tendency is make equal possibilities for man and woman raise every day an issue of need taking into account of “gender issue” on the high level of decision-making.

How policy issue on taking into account “gender issue” can enhance of nuclear security effectiveness? Does it has an impact? However, is it right for Nuclear Security? Main question that you hear from the people, when you talk about “gender issues” – “Are you talking about Feminism? We have no problem with any “gender issues”, we are very respect woman”. Those questions I received last year on the XV Ukrainian conference on physical protection, accounting and control of nuclear material, when we were decided what issues should be raise on the next conference.

2019 is very special year for Ukraine in nuclear security area from gender point of view. First, at first time “gender issue” will be raised of the Ukrainian conference 23-28 September 2019. Secondly in cooperation with Swedish Radiation Safety Authority, Ministry of Energy and Coal Industry of Ukraine and Kyiv Polytechnic Institute will be organized Woman in Nuclear Security Forum, October 15, 2019.

In the paper will be reflect the results of meetings, comparison with foreign partners, such as Sweden, USA, Canada of existing situation and analysis of impact of inclusion of “gender issue” to the policy of organization.

State
Ukraine

Gender
Female

Primary authors: KLOS, Nataliia (2004); MARTYNENKO, Hanna; Mrs ANDERSSON, Sarmite (Swedish Radiation Safety Authority)


Track Classification: CC: Nuclear security culture in practice with a focus on sustainability
Synergistic Regional Capacity Building Efforts on Nuclear Forensics in the GUAM Countries

The European Union and the United States have a long standing cooperation with the GUAM countries in the nuclear security area. For many years the European Commission’s Joint Research Centre (JRC) has been implementing cooperative projects with Georgia, Ukraine, Azerbaijan and Moldova related to countering nuclear smuggling, to improving national preparedness and to nuclear forensics. Similarly, the US DOE, through its National Nuclear Security Administration (NNSA) and the National Laboratories, operated projects related to enhancing technical nuclear forensics and inter-agency cooperation in GUAM countries. In recent years, JRC and the Nuclear Smuggling Detection and Deterrence program of NNSA implemented nuclear forensics related projects in partnership. This close coordination and cooperation enabled a better use of resources and ensured a coherent approach for training, for developing protocols and procedures, for promoting best practices and for conducting exercises.

Within the framework of the STCU (Science and Technology Center in Ukraine), a project set has been developed to support sustainable nuclear forensics capacity across regional partner countries as part of the region’s nuclear security culture. The project set is co-funded by the European Union and the United States and the implantation is supported and monitored by experts from JRC and NSDD. Within this project set, nuclear forensics subject matters experts from the GUAM (Georgian, Ukraine, Azerbaijan and Moldova) region participate in three STCU projects, and integrate new nuclear forensics experts as appropriate to the project.

The three projects cover:

- National nuclear forensics library (NNFL) development work, enabling GUAM countries to use available resources and international experience while maintaining the opportunity for a country-specific technical implementation of the NNFL;

- Technical work and training intended to bolster and sustain existing nuclear forensics expertise, and to extend regional and international collaboration; and

- Multifaceted project aimed at training the next generation of nuclear forensic scientists at the undergraduate, masters and doctoral levels.

The presentation will provide an overview of the implementation of the three projects, pointing out the additive synergies between project activities, and offer insights as to the benefits of regional capacity building work. Additionally, the paper will illustrate how these three projects build on achievements of previous activities and contribute to sustain nuclear forensic capabilities in the region; further improve the ability to investigate and prosecute perpetrators and to strengthen the nuclear security culture of the four countries.

State

Other

Gender

Not Specified
Primary authors: Mayer, Klaus (European Commission - Joint Research Centre, Institute for Transuranium Elements); Dallas, Liz

Co-authors: Dale, Debbie (US DOE Los Alamos National Laboratory); Galy, Jean (European Commission / Joint Research Centre); Iyer, Mansie (NNSA); Oujo, Kaitlin (U.S. Department of Energy)

Presenter: Dallas, Liz

Track Classification: MORC: Nuclear forensics
Effective Implementation of Tabletop Exercises for Nuclear Security

Ensuring a timely and effective response to a security event involving nuclear or radioactive material is a challenge. This is due to the need for accurate and reliable contingency plans and procedures, adequate coordination between stakeholders involved in response, and the costs of systematic exercises to validate, test, evaluate, and prepare personnel to respond to nuclear security events. Security tabletop exercises (TTX) offer a flexible and economic way to validate security response plans, strengthen staff competencies through training, and test well-established response procedures while assessing security personnel awareness and readiness.

The use of TTXs for the validation of contingency and response plans identifies procedural, resource, operational and strategic gaps. Embedding TTXs into the validation process can serve to ensure that plans, procedures and arrangements are up-to-date and aligned with the current operational environment. In this context, using TTXs for validation provides all stakeholders, including off-site response, with the opportunity to clarify roles and responsibilities in the response to a nuclear security event.

Implementing regular TTXs into established drill and exercise programs contributes to the sustainability and enhancement of security training programs. These TTXs provide security personnel with the opportunity to train utilizing validated plans, and to practice procedures, decision-making processes, and response arrangements. As such, security TTXs can enhance knowledge of plans, procedures and protocols, and identify areas of improvement for procedures, personnel, resources and equipment.

TTXs serve as an effective method to test specific scenarios within the design basis threat and can complement the force-on-force exercise program. A well-designed TTX can provide security metric data on the effectiveness of an organization’s response to a nuclear security event, while employing far less resources, financial cost and commitment than drills and full-scale force-on-force exercises. TTXs provide a safe environment to test and familiarize security, emergency and off-site response personnel with site plans, roles and responsibilities, incident command, and tactics to ensure a coordinated response. Implementing TTXs in the force-on-force exercise program can provide an objective assessment of security capabilities and will enable the early identification of vulnerabilities and operational and procedural gaps.

Through comparative analysis and benchmarking, this paper illustrates the effective implementation of regulatory requirements and guidance for security exercises, exercise models and approaches used by various IAEA Member States. This paper identifies good practices among domestic and international organizations in exercise development and execution. In addition, this paper provides suggestions and proposes options for the inclusion of additional requirements in a State’s regulatory regime.

State
Canada

Gender
Female
Primary author: FAHEY, Jessica
Presenter: FAHEY, Jessica

Track Classification: CC: Innovative technologies to reduce nuclear security risks and improve cost effectiveness, where feasible
Holistic smart products for nuclear security

Radiation detectors with fully integrated digital readout and Power-over-Ethernet (PoE) connectors enable a whole set of new applications and services. In this paper, neutron and gamma detectors will be presented which are read out by low-power Silicon Photomultipliers (SiPMs) that allow for long autonomy from mains power supply when deployed in the field. This is especially needed in applications where detectors are mounted on unmanned vehicles or drones, or in applications where networked devices are mounted to cars or relocatable detection systems.

The Power-over-Ethernet connector allows direct addressability of each detector by its IP address when several detectors are networked. This information flows into smart software solutions which take advantage of this feature to adjust machine learning algorithms. If GPS is also provided then a simple mapping of an area is obtained within a short timeframe.

Such rapid situational awareness is especially useful in case of a CBRNe incident or for intelligence services to get a clear picture of a site or environment. The information can also be provided to smart city networks.

The presented software ensures that limited training of operators is needed, which has an impact on the cost of an exercise. In addition, as PoE based radiation detectors are designed to be networked, all information can flow into an on-site or remote central alarm station where appropriate measures are taken to react in case of an alarm or anomaly.

The SiPM readout allows the presented gamma detector to be thinner than 2 cm and widely scalable in width. This feature is interesting for applications where limited space is available, for example for airports where the detectors can be integrated into existing layouts and walls to monitor passengers or luggage.

In addition to the many advantages fully digital radiation detectors provide during operations, PoE also allows simple plug and play maintenance concepts which will be presented in this paper.

State

Switzerland

Gender

Female

Primary authors: DAVATZ, Giovanna (Arktis Radiation Detectors Ltd); CHANDRA, Rico (Arktis Detectors); Dr GENDOTTI, Ulisse (Arktis Radiation Detectors Ltd); Dr PANNIELLO, Marco (Arktis Radiation Detectors Ltd)

Presenters: DAVATZ, Giovanna (Arktis Radiation Detectors Ltd); CHANDRA, Rico (Arktis Detectors); Dr GENDOTTI, Ulisse (Arktis Radiation Detectors Ltd)

Track Classification: CC: Innovative technologies to reduce nuclear security risks and improve cost effectiveness, where feasible
Global Material Security in 2020 – A Focus on the Future

The U.S. Department of Energy’s National Nuclear Security Administration (NNSA) works to reduce the global danger from weapons of mass destruction in the United States and internationally. NNSA’s international nuclear security programs began more than 20 years ago as a cooperative effort with Post Soviet States under the Cooperative Threat Reduction framework, and has evolved to its approach today that addresses enduring and emerging threats by engaging with a host of new partners, both governmental and non-governmental. In implementing these international efforts, NNSA brings the wealth of expertise that resides in the U.S. national laboratories to solve complex nuclear security challenges with our partners and supports the growth of peaceful applications of nuclear technology.

This presentation will discuss the evolution of NNSA’s nuclear materials security programs in the contemporary landscape and provide NNSA’s views on what a risk-informed, defense-in-depth approach to nuclear security looks like in 2020 and beyond. In 2015, DOE/NNSA’s Office of Defense Nuclear Nonproliferation (DNN) reorganized to address the changing threat environment in a flexible and comprehensive way. Since 2015, GMS has worked to integrate and streamline efforts to protect nuclear and radiological material, and to form a cohesive and balanced organization that operates as "one GMS." GMS works with partners worldwide to secure nuclear and radiological materials, and to interdict and investigate the trafficking of such materials. GMS, through its three offices – Office of International Nuclear Security, Office of Radiological Security, and Nuclear Smuggling Detection and Deterrence, provides nuclear and radiological security upgrade and related training, strengthens supporting regulations, inspections, and security culture, and provides a wide range of technical consultations looking at innovative security solutions. To address nuclear material out of regulatory control, GMS strengthens the capacity and commitment of partners to deter, detect and investigate illicit trafficking of nuclear materials and works with multilateral partners to strengthen the global detection architecture.

GMS is committed to capacity-building and sustainability, and seeks to build strong relationships with international partners to prevent the unauthorized acquisition of nuclear and radiological material, and to augment capabilities to detect and deter the illicit movement of such materials. GMS implements this mission against a backdrop of a constantly evolving threat environment, emerging technologies, and a growing demand for safe and secure peaceful nuclear technology. This demand is expected to continue, requiring sustained focus on nuclear safety and security to support the continued and expanded use of nuclear energy and other peaceful nuclear applications.
Primary authors: Mr ATKINS, Art (US DOE/NNSA); Mrs MAEGON, Barlow (US DOE/NNSA); Mrs VOGLER, Katherine (US DOE/NNSA)

Presenter: Mr ATKINS, Art (US DOE/NNSA)

Track Classification: CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
Given the rising threat of radiological and nuclear terrorism, it is imperative to assess if radiological facilities, such as universities and medical centers, have the means to fully understand and evaluate the security of their radioactive sources. In this context, risk assessment is a function of threat, vulnerability and consequences. This study aims to develop and demonstrate a methodology to compute a risk index for a higher education institution (university), based on the probability of occurrence of a Threat Event (TE) and its subsequent magnitude of incurred loss. This risk index provides a quantitative value for comparing risk and making decisions towards radiological security improvements. The index employs the triplet definition of risk, structured as a set of threats, vulnerabilities, and consequences. These were used to construct a single composite number by weighing the threat scenario probabilities, relative attractiveness and characteristics of the radioactive material, multiple parameters elevating vulnerability of source security, and the consequence net loss. The risk decomposition is based on the Factor Analysis of Information Risk (FAIR) ontology. Probability density functions and event trees were then used to simulate scenarios to estimate the probability of successfully completing a malicious act at the university, such as theft of the source. For this study, a higher education institution that uses a number of radioactive materials for research and teaching, was analyzed using the risk index model. Specifically, three facilities housing nuclear or radioactive sources at the university were compared: a research reactor, Co-60 irradiator, and radiopharmaceutical laboratory. The emphasis of the study is on the research reactor, but the other facilities were also analyzed for comparison. The research reactor facility houses a 10-kW swimming pool type reactor containing plate type uranium/aluminum fuel. The irradiator facility contains both Co-60 and Cs-137 sources with Ci amounts of activity. The radiopharmaceutical facility contains a number sealed and unsealed sources with mCi amounts of activity. Two proposed attack scenarios (theft and sabotage) were simulated for each facility. The radiopharmaceutical laboratory sources yielded the highest probability of successful sabotage and theft outcomes while the reactor facility yielded the highest consequences in the sabotage scenario. The contribution of the proposed research is significant as it allows for a new tool in the field of radiological source security—one that is expected to introduce, analyze and numerically test a methodology that yields a facility level risk index.

State

United States

Gender

Male

Primary authors: HARRIS, Jason (Purdue University); RANE, Shraddha (Purdue University); Ms SHEFFIELD, Courtney (Purdue University)
Presenter: HARRIS, Jason (Purdue University)

Session Classification: Research Reactor Security

Track Classification: PP: Research reactor security
Sri Lankan Experience on Security of Radioactive Materials in Transport from a Regulator’s Perspective

The Sri Lanka Atomic Energy Regulatory Council (SLAERC) [successor of Sri Lanka Atomic Energy Authority] was established on 01st of January 2015 by the Sri Lanka Atomic Energy Act No. 40 of 2014 (Act), with the mandate of establishing and implementing a regulatory regime for ensuring the protection of public, patients, radiation workers and the environment from potentially harmful effects of ionizing radiation and security of radioactive sources. The fulfillment of the mandate of the Act, SLAERC empowered for licensing & inspection of users of radiation applications, control of import & export of radioactive materials, management of radioactive waste, ensuring physical protection of radioactive materials, developing the capability to respond to nuclear or a radiological emergency, meeting the obligations of Sri Lanka under the safeguards agreement with the International Atomic Energy Agency (IAEA) and the establishment of the legislative and regulatory framework necessary for the above.

Sri Lanka uses high activity category 1 radioactive sources for medical, industrial & research applications such as radiotherapy machines, pool type & self-shielded irradiators in 11 locations across the country. The physical protection systems have been installed for all these locations against theft, sabotage or other malicious acts of these radioactive sources as national nuclear security requirement included in the Act under chapters of ‘Safety and security of radioactive materials & Physical protection of radioactive materials’

Implementation of regulatory requirements and enhancing a nuclear security regime are important to protect radioactive material while in transport against theft, sabotage or other malicious acts that could, if successful, have unacceptable radiological consequences. Therefore, the SLAERC (Competent authority for regulating transport of radioactive material in Sri Lanka) has taken several steps for the regulatory implementation of security issues in the transport of category 1 sources to the above 11 locations.

Almost all the required radioactive sources are imported including category 1 sources as no radioactive source production facility is available in Sri Lanka. Therefore, the usual route of this category 1 source transportation is done from relevant sea port or airport to the consignee’s destination (licensee’s premises) and re-exportation of decayed sources from licensee’s premises to the relevant port in the country.

The SLAERC coordinates provision of security for these category 1 sources during transport in collaboration with Police Special Task Force (STF) and Sri Lanka Police. The prior arrangements of customs & port clearance are arranged immediate delivery just after arrival of the ship / flight. SLAERC inspect the radioactive package at the relevant port in appropriate way in order to conform completeness & correctness and seal the container and supervise the entire transportation.

If the packages are needed to be stored in any location in transit, prior to transport the final destination, an approval should be obtained from SLAERC. This approval is given after verifying the adequacy of availability of security in such location. Proper security arrangement is provided during such transit and at the consignee’s destination until sources loaded to the relevant irradiator or radiotherapy machine.

A tracking device (T-Star or track lock) supplied by the Oak Ridge National Laboratory under the United State Department of Energy (USDOE), Global Material Security (GMS) program is used in these whole transportation activities. Information of exact location of the transport container can be obtained by this instrument while transporting the consignment.

Before issuing the licences for these transportations, the SLAERC obtained all information of personnel engaged in the transportations for prior assessment of their trustworthiness, information of
vehicles to ensure their conditions for safe and secure transport of materials and security provided to the sources during transport.

SLAERC organized a transport security table top exercise also for transport of category 1 sources to train the persons involved in this field (response forces & transporters of radioactive sources) with the assistance of USDOE under GMS program. This simulation type table top exercise was most beneficial to all the participants to obtain the hands-on experience of the real scenarios.

At present one of the challenge in transport of radioactive materials is promulgation of national regulations on transport of radioactive materials including safety & security aspects. The preparation of this regulation is also a requirement of section 87 of the Act. Preparation of transport security plan and human resource development in SLAERC & other relevant personnel (training & awareness of the personnel involving in transport activities) are other challenges for safe & secure transport of radioactive material program in Sri Lanka.

However, in the midst of such challenges SLAERC has successfully conducted all category 1 transport security events up to now. In the future SLAERC expects to carry out such transportation more effectively & efficiently in accordance with the international standards by implementing the identified future plans and overcoming the above challenges.

**State**

Sri Lanka

**Gender**

Male

**Primary author:** Mr DE SILVA, Uththama Wadu Kapila Haryantha (Sri Lanka Atomic Energy Regulatory Council)

**Presenter:** Mr DE SILVA, Uththama Wadu Kapila Haryantha (Sri Lanka Atomic Energy Regulatory Council)

**Track Classification:** CC: National nuclear security regulations
Complex spectra analysis of peaks interference through gamma-ray spectrometry of U-235, Ra-226 and Th-234

Natural radioactivity is unevenly distributed in the terrestrial environment, depending on the rocky nature of the soil. It can be dangerous for human life at a certain concentration of radionuclides. Unfortunately, these radionuclides are imperceptible to the human senses and detectors are used to "observe" them. In Burkina Faso, there are localities where the radioactivity is relatively higher than elsewhere. In these High Background Radioactivity Areas (HBRAs), studies have to be performed to determine the exact level of radioactivity in order to deduce the possible risks for the residents as well as those of neighboring localities where soil could be transported. There could have some nuclear security issues according to the nature of the transported materials which can involved illicit trafficking at borders. So appropriate detection measures are requires for detecting and identifying crucial threats in order to make difference between materials from real threat such as HEU and which one from innocent circumstance like NORM. RPM, identiFinder, inSpector 1000, PRD and Radeye are some efficient and appropriate devices for the use on field to detect radioactivity. For that nuclear security issue, it is very important to have accurate result of activity measurement which can be used to evaluate the radiological hazards. For this reason, the specific activity of U-238, U-235, Ra-226, Th-232 and K-40 have to be determined. Unfortunately, there is a lack of precision in the quantification of these nuclides. This is due to the complexity of the involved peaks. Indeed, the deconvolution process is faced to the peak interference phenomena of the spectra analysis. In fact, the direct detection of Ra-226 by gamma-ray spectrometry method is done by using its ionizing radiation emission energy of 186.211 keV. For the U-235 the most probable emission of energies are 185.720 keV and 143.767 keV. These radionuclides have their peaks so close that their respective peaks resolutions do not make it possible to distinguish them. Thus, the quantification of U-235 is increased by that of Ra-226 and vice versa. One solution used to overcome this issue is based on the secular equilibrium of the U-238 series. Since the proportions are well known between the isotopes of uranium, and the concentration of Ra-226 is equal to that of U-238, it is possible to find an acceptable estimation of the activities of Ra-226 and U-235. However, in a given sample, one cannot really ensure that the proportions have remained intact between the isotopes of uranium. The complexity remains in the quantification of these radionuclides and that of Th-234. This last one is used to determine the activity of the U-238 and unfortunately, it has two peaks of 92.38 keV and 92.80 keV energy extremely close to each other, also facing the interference phenomena which remains a real challenge. Fortunately, innovative calculation techniques, new algorithms and tools could provide a solution. In this study, methods and results for gamma spectra analysis using commercial and open-access tools will be compared and discussed. It is brought on this paper, a solution for solving the interference phenomena problem based on these tools. These new methods will be used to analyze the spectrum of a sample from a HBRA. The activity of U-235, Ra-226 and Th-234 will be calculated with acceptable accuracy.

State
Burkina Faso

Gender
Male

**Primary author:** BEOGO, Cedric Elisée (ARSN)

**Co-author:** Ms CHAIRAM, Issariya

**Presenters:** BEOGO, Cedric Elisée (ARSN); Ms CHAIRAM, Issariya

**Track Classification:** CC: Advances in nuclear security research and development; international cooperation on nuclear security research
Drafting regulations for transport safety and transport security achieve two separate objectives, which can lead to divergent outcomes. With transport safety, the goal is to protect the public from the effects of ionizing radiation, while in contrast, the goal of transport security is to protect the material from malicious actors. While many Member States may have transport safety regulations for radioactive materials, transport security regulatory development is still in its nascent stages globally. Trying to develop harmonized transport safety and transport security regulations could lead to challenges ranging from differences in terminology used in transport safety versus terminology uses in transport security, roles and responsibilities for the variety of stakeholders involved in transport, and finally, the possible role of multiple competent authorities in governing the transport of dangerous goods, such as radioactive materials. While the International Atomic Energy Agency (IAEA) is currently developing a process of a methodology for drafting transport security regulations for nuclear and other radioactive materials, any process must address both safety considerations and security requirements. As the most vulnerable part of the life cycle of radioactive materials, the need for harmonized transport safety/transport security regulations is essential. This paper investigates the regulatory elements of the safety-security interface for nuclear and other radioactive material in transport. Examining challenges including use of terms, the role of multiple competent authorities, and practical challenges involved in the safe and secure transport of radioactive material, the paper analyzes the need for integrated regulatory development for the safe and secure transport of these materials.
Preventing a Dirty Bomb: Case Studies and Lessons Learned

Today, tens of thousands of high activity radioactive sources are used in over 100 countries. They are used in medicine, industry, agriculture, academic, and government facilities for a variety of beneficial purposes. Many of these sources are poorly secured, vulnerable to mishandling or even theft by terrorist organizations seeking the materials needed for a radiological dispersal device (RDD), often referred to as a “dirty bomb.” Cesium-137 is of particular concern, as it the most dangerous radioactive material that can be used in a (RDD). The economic impact of a Cesium-137 bomb explosion could be in the order of tens of billions of dollars.

The purpose of this paper is threefold. First, we propose a shift in paradigm, from a security perspective geared towards risk reduction to a public health approach invested in risk elimination. We are currently at a moment where new technologies can safely and effectively replace many Cesium-137 devices with equal or even improved outcomes. This is certainly the case with blood irradiation devices, where the consensus on the benefits of x-ray irradiators have led several countries to eliminate their use and others to prioritize their replacement. The marketplace in many countries has already seen the uncoordinated and voluntary replacement of Cesium-137 for blood irradiation. Similarly, there is growing consensus that x-ray devices can meet and exceed medical and research goals of Cesium-137 devices for a wide range of uses. The paper will provide a brief overview of the current state of efforts that aim at eliminating the use of Cesium-137 irradiators for blood sterilization and research, including interviews with blood bank operators and research scientists who have adopted the new technologies successfully in their programs.

Second, in the absence of regulatory requirements, this paper will propose a model for achieving voluntary permanent threat reduction at institutions within major urban areas. The paper will highlight factors that encourage voluntary replacement of Cesium-137 devices, identify key roles played by regulators and decision makers at different levels of government in implementing Cesium-137 substitution strategies. The paper will highlight the incentives, challenges, and information gaps that shape decisions to adopt a public health paradigm for managing the inherent risks of Cesium-137 irradiators. To this end, the authors will argue for the creation of an “advocacy network” of organizations and individuals committed to cesium replacement. This network would facilitate collaboration and share experiences amongst users and create informal channels for distributing information on latest technological advances, practical experiences with converting to alternative technologies, comparative research studies, and fiscal implications of converting to devices that pose no terror risks. The network would also provide assistance to those navigating the process of technological substitution by tracking and documenting regulatory changes and voluntary substitution efforts across the globe; supply the necessary infrastructure to coordinate voluntary threat elimination efforts across institutions, regions and national governments; and serve as the public facing clearing house of efforts aiming to eliminate risks through the use of alternative technologies.

Thirdly, the paper will recommend that IAEA Member States encourage the IAEA to promote alternative technologies to radioactive sources and provide guidelines that support States in their implementation of INFCIRC/910 on the Joint Statement on Strengthening the Security of High Activity Sealed Radioactive Sources. While there are clear viable alternatives for Cesium-137 irradiators, more research is needed to develop equivalent alternatives for other radiation sources. The authors believe that IAEA Member States should encourage the IAEA to promote and support research efforts on the development of technically and economically realistic and acceptable
non-HASS technologies, incorporating in these efforts the manufacturers, end-users, standards-setting bodies, and technical experts. IAEA engagement on alternative technologies could include formally incorporating alternative technologies into key planning documents such as the next Nuclear Security Plan, coordinating the development of standards and guidance for alternative technologies, and facilitating sharing of information related to alternative technology to support the decision-making of operators, regulatory bodies, and other competent authorities. In a world where there are heightened concerns about radiological terrorism as well as increased requests by Member States for access to effective cancer care, alternative technologies can simultaneously support public health needs and risk elimination to build a healthier, more secure world.

**State**

Other

**Gender**

**Primary authors:** Ms ILIOPULOS, Ioanna (Nuclear Threat Initiative); Mr BOYD, Christopher (Nuclear Threat Initiative); Ms BUFFORD, Jessica (Nuclear Threat Initiative)

**Presenter:** Ms BUFFORD, Jessica (Nuclear Threat Initiative)

**Track Classification:** CC: Innovative technologies to reduce nuclear security risks and improve cost effectiveness, where feasible
Investigation of the rare-earth element pattern of uranium oxide (U3O8) for attribution of uranium in safeguard and nuclear forensics environment

Illicit trafficking of radioactive material and especially nuclear material (thorium, uranium, and plutonium) has been an issue of concern since the beginning of the 1990s, when the first seizures of nuclear material were reported to the International Atomic Energy Agency. In this work, twenty samples selected for investigation originate from South Africa and Namibia uranium mines. The aim of this study was to determine whether the rare-earth elements patterns measured in a particular sample can be used to attribute the sample to the production or reprocessing plant. Rare earths elements (REE) are a set of seventeen chemical elements in the periodic table, specifically the fifteen Lanthanides with the addition of scandium and yttrium.

The REE share numerous common physical and chemical properties that make them difficult to chemically separate from each other. The atomic number (Z) for these REE metals range from 57 to 71 and they are divided into two sub-groups, namely the light rare earth elements (LREE) and the heavy rare earth elements (HREE). The LREE consists of the following metals namely, lanthanum (La), cerium (Ce), praseodymium (Pr), neodymium (Nd), promethium (Pm), samarium (Sm), europium (Eu) and gadolinium (Gd). The HREE include metals such as terbium (Tb), dysprosium (Dy), holmium (Ho), erbium (Er), thulium (Tm), ytterbium (Yb) and lutetium (Lu).

A large amount of uranium is found in rare earths deposits, and may be extracted as a by-product. As a result, REE in uranium compounds can be used as an evidence of uranium origin. In this study, REE was measured in the uranium oxide (U3O8) collected from South African and Namibian gold mine. Measurements were carried out using an inductively coupled plasma mass spectrometer (ICP-MS) NexION 2000. The results for the Namibian mine show the REEs exhibit light REE-enriched patterns with pronounced positive Ce anomaly when normalized to chondrite which indicates that the REEs are taken up in proportion to their relative concentration in the source rocks. While for the South African mine, the REEs exhibit heavy REE-enriched patterns with pronounced positive Tb anomaly when normalized to chondrite. These results confirm that, REE patterns used for origin location do reflect significant variation within mine and thus provide valuable information about the geochemical formation and origin.

State
South Africa

Gender
Female

Primary authors: Mr KUPI, Tebogo Gilbert (North-West University Mafikeng); Ms MOKHINE, Naomi Dikeledi (North-West University Mafikeng); Prof. MATHUTHU, Manny (North-West University Mafikeng)

Presenters: Mr KUPI, Tebogo Gilbert (North-West University Mafikeng); Ms MOKHINE, Naomi Dikeledi (North-West University Mafikeng)
Track Classification: MORC: Nuclear forensics
Open-Source vs. Proprietary Software: A Case Study in Trust and Security

Software plays an ever-increasing trusted role in all aspects of life: from door locks to self-driving cars to fish tanks. We† trust the software in our smart locks to keep intruders out of our houses. We† trust the software in self-driving cars to get us to our destination safely. We† even trust the software in our smart fish tank to feed our goldfish. The software running nuclear facilities is no exception, it requires trust – trust in the functionality, trust in the quality, trust in the security etc. As the use of digital systems continues to rise in nuclear facility systems, trust in the software powering those systems plays an increasingly important role in nuclear security.

In this paper we examine the trustworthiness and security of open-source vs. proprietary software. As open-source software has grown and become mainstream, there is now often a choice between an open-source and a proprietary solution. We attempt to enumerate the advantages and disadvantages of each, particularly with respect to trust and security. In order to do that, we define each in terms of licensing models, source release models, development models, business models and so forth. We discuss how each variable impacts trust and security. Finally, we present a case study in the software powering virtual private network (VPN) devices, important network security components specifically recommended for nuclear security applications in the International Atomic Energy Agency’s (IAEA) Nuclear Security Series 1 and in a report to the United States (U.S.) Nuclear Regulatory Commission (NRC) 2 regarding security at nuclear power plants.


†Perhaps, more accurately, “some of us”.

State

United States

Gender

Primary authors:  MORGAN, Keith S. (Los Alamos National Laboratory); GRAHAM, Paul S. (Los Alamos National Laboratory)

Presenter:  MORGAN, Keith S. (Los Alamos National Laboratory)

Track Classification:  CC: Information and computer security considerations for nuclear security
An Innovative Mobile Hot Cell with Remote Handling Capabilities

Radioactive sources are used around the world to support life-improving and lifesaving industries. However, if found in the hands of terrorists and terrorist supporting organizations, these sources could be used to harm people and the environment. This paper will discuss the overall design, transportation configuration, deployment features, required equipment, personnel, and device interfaces of an innovative mobile hot cell with remote handling capabilities. This new hot cell design will provide facilities that have limited radioactive materials handling infrastructure the means of securing their radioactive sources by consolidating and packaging for end-of-life management in a secure and safe environment. The design and advanced features of this hot cell can be deployed in remote locations; will improve the basic assembly, operation, and disassembly of a mobile system; and provide a measurable improvement in security, through a reduction in deployment time and handling efficiencies, compared to current mobile hot cell designs. Improvements in assembly and disassembly are achieved by using prefabricated nesting biological shields that are placed around the inner hot cell only to a thickness necessary for the specific activity of the material being handled. Reconfigurable robotic arms and three-dimensional camera systems are used to improve the handling efficiencies within the hot cell compared to current mechanical manipulators and leaded glass or zinc bromide windows which cannot be reconfigured and offer limited visibility. As a result, these improvements can lower security risks associated with disused radioactive sources found in public industries by making it more likely local stakeholders invest in removing, consolidating, and packaging for end-of-life management. Two ways this might be achieved is by 1) reducing operational costs from staff time and equipment, thereby reducing the financial burden on stakeholders and increasing the likelihood material removals will occur, and 2) minimizing opportunities for bad actors to target a removal or consolidation operation by significantly decreasing the time it takes to complete the process from assembly to final transportation. In addition, with the use of remote handling and three-dimensional cameras, hot cell users can significantly lower radiation exposure by extending the interface distance between the operator and the hot cell. By reduced operation time at a single location, hot cell users can efficiently complete multiple removals and eliminate the need for frequent visits to the same location, which may decrease the risk for malicious tracking of repetitive operations. Finally, human operational error from fatigue due to repetitive tasks can also be reduced by pre-programing routine tasks.

The innovative design and advanced features of this new hot cell with remote handling and three-dimensional vision capabilities provide for an integrated but independent set of systems that can streamline logistics, allow for greater flexibility in use, such as equipment reconfiguration and mission modifications, and provide a capability to enhance the security of international source end-of-life management.
Co-authors:  Mrs MCBRIDE, Kathryn (Idaho National Laboratory);  Mr KENNEY, Kevin (Idaho National Laboratory);  Mr EGAN, Steven (Idaho National Laboratory)

Presenter:  Dr WRIGHT, Christopher (Idaho National Laboratory)

Track Classification:  MORC: Coordinated response to nuclear security events
Applying Nuclear Forensics in Nuclear Material Accounting and Control of Radioactive Material out of Regulatory Control from a Facility

Nuclear forensic has found a niche in Nuclear Security and a tool for attribution evidence. This is normally applied when nuclear material gets out of regulatory control and then interdicted. Nuclear Forensics provide a laboratory technique for material accounting and control. The signatures can be in the form of Nuclear material age dating, Lead isotopic ratios, Nuclear material processing mechanism (impurity data), sample morphology or a combination of at least any two of the above. At the Center for Applied Radiation Science and Technology, we used both Gamma spectrometry (High purity Germanium Detectors) and ICP-MS (NexION 2000), to resolve the nuclear forensics signatures of a Uranium Ore Concentrate (Yellow cake). The aim of the research was to determine the nuclear forensics signatures of a yellow cake powder for attribution. The objective is to provide a systematic validated Nuclear Material accounting and control that answers to the question of interdicted materials out of Regulatory control.

First recovery processing water yellow cake production stage of the Processing Plant was analyzed by ICP-MS Uranium Provenance and age of the ore sample before crashing. Results show that the Recovery Process water from has a Uranium ranging from $(145.68 \pm 33.43) \text{ mgL}^{-1} (1.81 \pm 0.41) \text{ kBqL}^{-1}$ to $239.54 \pm 22.78 \text{ mgL}^{-1} (2.97 \pm 0.28) \text{ kBqL}^{-1}$, at the Processing plant. Thorium levels were at mean concentration of $(16.88 \pm 2.48) \text{ µgL}^{-1} (0.21 \pm 0.03) \text{ BqL}^{-1}$.

The absence of Ca, Mg, Al, Mn, Fe, Na, Zn and Cd shows that the Mine does not utilize acid leaching as its uranium processing mechanism (leaching). In acid leaching, the oxidation of the uranium compounds is typically achieved using manganese dioxide (MnO2), sodium chlorate (NaClO3), and Fe(II) salts. The major impurities are iron, thorium, phosphate and rare earths, molybdenum as well as zirconium. Other major impurities include thorium, vanadium, phosphate and sulphate. The high levels of Vanadium with a mean value of $(125.88 \pm 0.68) \text{ mgL}^{-1}$; Cr, As $(0.384 \pm 0.038) \text{ mgL}^{-1}$, Se $(0.030 \sim 0.096) \text{ mgL}^{-1}$, and Mo $(0.471 \pm 0.030 \text{ mgL}^{-1})$ indicates that the Mine operators used alkaline leaching followed by hydrogen peroxide to remove the high concentrations of Vanadium and Molybdenum.

Selenium and Uranium increased linearly (strongly correlated) with the Sample ID. Then we determined the lead isotopic ratios of the yellow cake from the same batch of samples, which was then used to calculate the age of the original sample and found to be around 1.3 Ga yrs. This is expected as the yellow cake investigated was from an Open pit uranium mine, which are characterized by younger ore deposits.

Finally, we evaluated the REE Signature patterns from the two process stages (Ore and yellow cake). Results show that in the ore the REE patterns are all the LRREE are depleted by the Acid processing mechanism of the mine, except Ce which is much high. The HREE are however slightly enriched towards Lu, showing very minimal fraction of the HREE due to processing. The observed deviations may be due to heterogeneous distribution of REE in different mineralogical phases (such as phosphates) in some CI-Chondrites.

We concluded that
i. analyzing the recovery process water gives distinct indicators of impurities that are in the ore. Hence the solvent extraction process can be decided upon (eg. alkaline leaching followed by hydrogen peroxide),
ii. Calcination of the Uranium precipitate needs to be done to remove Vanadium and other similar impurities.

May 9, 2020
at least three different nuclear forensics signatures could be clearly resolved by ICP-MS, viz: Processing mechanism, REE patterns and the age of the samples.

State
South Africa

Gender
Male

Primary authors: Prof. MATHUTHU, Manny (Center for Applied Radiation Science and Technology (CARST) North West University (Mafikeng)); Mrs UUSHONA-MIKA, Vera (National Radiation Protection Authority of Namibia)

Presenters: Prof. MATHUTHU, Manny (Center for Applied Radiation Science and Technology (CARST) North West University (Mafikeng)); Mrs UUSHONA-MIKA, Vera (National Radiation Protection Authority of Namibia)

Track Classification: MORC: Nuclear forensics
Strengthening National and International Plutonium Management Approaches

This paper discusses issues relating to separated plutonium (otherwise known as unirradiated plutonium) in civilian nuclear programs, that is, plutonium that has been chemically separated from spent nuclear reactor fuel by reprocessing but has not been reintroduced into a nuclear reactor after separation and subjected to further irradiation.

In those states that proceeded with civilian reprocessing programs, stocks of separated civilian plutonium have continued to grow in the aggregate. Taken together today, they are substantially greater than worldwide military plutonium stocks. Multiple approaches to limiting the separation of civil plutonium have been implemented, and still others have been given serious study, but stocks have increased regardless, while options for working down these stocks appear to be diminishing. Meanwhile, concern has deepened over the possible theft or diversion of this material, which could bring weapon-sufficient quantities of plutonium into the hands of violent extremists.

It is not sufficient simply to place reprocessing facilities and plutonium holdings under IAEA safeguards. Safeguards are not designed to address nuclear-material security issues. Accordingly, there is a need not only to address specific security measures for separated plutonium, but to complement these with institutional and technical measures to mitigate risks from separated plutonium.

These measures include steps to:

Limit existing reprocessing programs and their risk

• Political measures:
  o Encourage Japan to continue its reprocessing moratorium at least until the Rokkasho mixed plutonium and uranium oxide (MOX) fuel-fabrication facility is operational and a significant number of Japanese nuclear power plants licensed to burn MOX come back online; and to more seriously consider dry cask storage as an alternative to reprocessing.
  o Develop strategies to encourage France to shift to greater use of non-plutonium-based low-enriched uranium fuels for its domestic nuclear power plants and to refrain from exporting a reprocessing plant to China.

• Technical measures:
  o Where possible, reactors should be operated to avoid producing plutonium at or near weapon-grade. Where such material is produced, and reprocessing cannot be avoided, such material should not be reprocessed separately but blended in-process to avoid a product at or near weapon-grade.
  o Minimize the number of sites with separated plutonium holdings and the number of transport movements of separated plutonium and conduct regular reviews of the security of such sites.
  o Acknowledge permanent disposition of separated civil plutonium as a problem common to all states possessing significant quantities of this material and establish a new multi-state forum or expand the mandate of an existing forum to develop strategies for the permanent disposition of civil plutonium.
  o Re-examine international plutonium storage concepts.

• Technical measures:
  o Minimize the number of sites with separated plutonium holdings and the number of transport movements of separated plutonium and conduct regular reviews of the security of such sites.
  o Accelerate and maximize mixing of separated plutonium with uranium and conversion to more-processed forms—MOX pellets and fuel assemblies—even if the product will go unused for an extended period. Consider extending this mixing to include plutonium insufficiently pure to be
burned in reactor fuel and constructing a new fabrication line at La Hague, France, and using the existing facility at Sellafield to produce such impure MOX.

- For countries with large stores of MOX and MOX unlikely to be burned in the near term because of impurities, consider placing these fuel rods in the same dry casks as highly radioactive spent fuel rods, providing a medium-term storage capability that will be difficult for non-state actors to exploit, pending ultimate disposal.
- As the United States pursues its "dilute-and-dispose" option for the permanent disposal of excess military plutonium United States should share its dilution and packaging technologies with other states and include them in unclassified aspects of ongoing US research and development activities.

Discourage new reprocessing programs
- Sustain current technology controls
- Continue current restraints on transfers of reprocessing equipment and technology.
- Continue to pursue additional commitments like those in the US–UAE and US–Taiwan nuclear agreements, where the US partners have agreed to renounce reprocessing into the indefinite future.
- Actively promote dry cask storage technology as an alternative to reprocessing

**State**

United States

**Gender**

Male

**Primary authors:** Mr CARLSON, John (Nuclear Threat Initiative); Mr SPECTOR, Leonard (James Martin Center for Nonproliferation Studies); Mr POMPER, Miles (James Martin Center for Nonproliferation Studies)

**Presenter:** Mr POMPER, Miles (James Martin Center for Nonproliferation Studies)

**Track Classification:** PP: Nuclear security of nuclear fuel cycle facilities: emerging technologies and associated challenges and complex threats
A CO-ORDINATED RESPONSE TO NUCLEAR SECURITY EVENTS – CHALLENGES AND OPPORTUNITIES

29 May 2019

A CO-ORDINATED RESPONSE TO NUCLEAR SECURITY EVENTS – CHALLENGES AND OPPORTUNITIES

1. SUMMARY

Nuclear Security Events (NSEs) represent serious risks to the public and responding services alike and are extremely complex situations to resolve. It is essential therefore that States have a clear framework to deal with all aspects of those risks and that supporting plans facilitate the effective joint-working of multiple-agencies. The IAEA will publish formal guidance on this issue shortly. This paper is intended to share experiences gained so far during the development of that guidance in designing, delivering and sustaining capabilities required to provide an effective multi-agency response to NSEs.

1. CHALLENGES

Several workshops at national, regional and international level have been delivered to Member States (MS) during the development of the National Framework guidance. Without exception, those MS which have received the workshops have commented positively on the added value provided by having a well-structured and clearly defined national framework for dealing with NSEs. A number of challenges have been identified by MS during the workshops and some options for facing up to those challenges considered.

- Joint planning: responding services are very capable of developing plans to deploy their own response capabilities to the scene of an NSE. However, there is often a reluctance to participate in joint agency planning sessions as this implies a loss of control. The workshops were able to convince delegates of the vital importance of joint planning and the development of multi-agency concepts of operation which are necessary to deliver a joint plan.

- Ownership of the planning process and the response: unless the organisational hierarchy is clearly identified and formally agreed by all stakeholders, it is likely that levels of commitment from stakeholders will be sub-optimal or, even worse, the command and control arrangements lose clarity and become confused.

- Capability development: a particular challenge has been an undue focus on the procurement of detection equipment without an associated deployment strategy, a clear understanding of the limitations of the equipment, or trained and equipped personnel who can interpret the output of the equipment and take appropriate action without delay.

- Sustainability: it is inevitable that threat levels will vary over time and it is, of course, hugely expensive to develop a capability which can respond to a high threat environment. However, MS can be tempted to make economies in sustaining the level of the response as soon as the threat level appears to diminish. If this is done without agreeing a sensible baseline capability which can be easily maintained and quickly upgraded, and without a knowledge management strategy which prevents expertise from being drained away and not replaced, MS can easily find themselves unprepared to meet emerging threats. This often leads to constant re-learning of the same lessons by organisations, with a vicious circle of capital investment followed by premature scrapping of equipment and a further round of expenditure when the response falters during the next incident.

3. OPPORTUNITIES

Some potential solutions have been identified during the workshops which expand on the formal guidance. There are some non-complex opportunities for improving the quality of the response to NSEs.
• Joint planning and exercising develops relationships which will be of critical importance during an NSE. The level of trust generated between individuals during joint activities cannot be overstated. True interoperability comes when the responding agencies understand not only their role but also the roles of the other agencies working alongside them.

A graded approach to the management of risks, when adopted by the responding agencies, facilitates a shared understanding of the problem, a joint evaluation of the hazards and a shared approach to their management.

• The National Framework guidance rationalizes the key activities and outcomes necessary for a response to be effective. These can then become part of a joint concept of operations linked to a set of strategic priorities. In that way there is a clear “line of sight” from strategic command through to the front-line response operation.

• The benefits of the collaboration on planning for, and dealing with, NSEs can flow into the planning process for the response to other types of security event, not only those involving the potential or actual release of radiation.

• Lessons from joint training and exercising -'red-teaming’ for example - can be fed back to protective security planners and assist in identifying the vulnerabilities which led to material becoming out of regulatory control in the first place.

1. CONCLUSION The value of a National Framework for response to NSEs is clear – addressing the complexities of planning and responding to NSEs jointly with partner agencies brings benefits which reach beyond nuclear security.

John Edward Jones O.B.E.
Independent Consultant
UK
john@jejones.co.uk

State
United Kingdom

Gender
Male

Primary author: Mr JONES, John Edward
Presenter: Mr JONES, John Edward

Track Classification: MORC: Coordinated response to nuclear security events
Switching from a Cesium-137 Blood Irradiator to an X-ray Irradiator – Experience at a Community-based Hospital in the Northeastern U.S.

Monday, 10 February 2020 15:00 (15 minutes)

Blood Irradiators are often used to irradiate blood and blood components prior to transfusion to prevent the proliferation of certain types of T lymphocytes that can inhibit the immune response and cause graft-versus-host disease. Morristown Medical Center, which is part of Atlantic Health System based in the northern part of New Jersey, USA, employed a Cesium-137 Blood Irradiator for about 20 years.

On November 14, 2005, the U.S. Nuclear Regulatory Commission (NRC) issued Order EA-05-0902, imposing increased controls for certain high-risk radioactive materials such as those contained in the Blood Irradiators. On December 5, 2007, the NRC issued Order EA-07-3053, imposing fingerprinting and criminal history records check requirements for unescorted access to certain radioactive material. These increased control (IC) requirements were imposed on radioactive materials of concern such as Cesium-137 (Cs-137) with activities greater than or equal to 27 Ci (1 TBq).

During the time of the IC orders, Morristown Medical Center’s Blood Irradiator contained approximately 1400 Ci (52 TBq).

Security enhancements, as well as response protocols were set in place, in order to comply with the USNRC Increased Control Orders, as well as 10 CFR 37. These included, but were not limited to, “trustworthiness and reliability” background checks, fingerprinting, FBI identification, criminal history records check, reinvestigation every 10 years for any individual with unescorted access, establishment of security zones and continuous physical barriers, continuous monitoring and detection of all unauthorized entries into security zones, and initial and annual training for the Security staff and Local Law Enforcement Agencies.

The facility eventually came to the decision to replace the Cesium irradiator with an X-ray Irradiator. Factors such as irradiator performance, prohibitive regulations, security issues and cost savings, that affected the decision, will be elaborated on. It is worth noting that the switch from a Cesium irradiator to an X-ray irradiator resulted in a quicker turnaround time and increased irradiation capacity per unit time, among other advantages.

A few factors that typically deter facilities from switching to X-ray technologies, will be discussed. These factors are generally rendered obsolete by updated technology as well as outweighed by the incurred advantages of switching.

Finally, a visual description of the day when our Cesium Irradiator was picked up for disposal, will be presented.

It is hoped that our experience will engage other facilities to do the same in terms of replacing their Cs-137 irradiators with technologies that yield better performance and result in much less vulnerability from theft and sabotage involving high-activity radioactive materials.

State
United States

Gender
Female

**Primary author:** HERNANDEZ, Marissa (Atlantic Health System - Morristown Medical Center)

**Presenter:** HERNANDEZ, Marissa (Atlantic Health System - Morristown Medical Center)

**Session Classification:** Innovative technologies to reduce nuclear security risks and improve cost effectiveness, where feasible

**Track Classification:** CC: Innovative technologies to reduce nuclear security risks and improve cost effectiveness, where feasible
Implementing a Counter Unmanned Aircraft System Program at a high-security nuclear facility

Implementing a Counter Unmanned Aircraft System (CUAS) Program at a high-security nuclear facility is a challenge and requires a certain degree of empathy toward system owners as you migrate toward planning, installation and final operational status. Resistance and conflict will arise during the project lifecycle. An appreciation for the level of dedication and concern demonstrated by owners of existing safety/security systems is critical. The installation of CUAS will most likely be placed on an expedited schedule once the decision to implement the program is made by leadership. Assembling the correct teams and working in a collaborative manner will lead to project success. CUAS implementation does not have to be cloaked in darkness. Many of the commercially available systems utilize technology that has existed for many years. Collaborating with other system owners will allow for CUAS integration into existing security infrastructure and provide a greater defense-in-depth strategy. Providing Subject Matter Experts (SME) who are not affiliated with the project will add value and integrity to any recommendations or opinions regarding concerns and potential impacts. All attempts to resolve safety and security concerns should be exhausted before energizing the CUAS. Early interaction with Safety Basis and Cybersecurity SMEs will benefit project timelines and avoid redundancy. Tactics associated with presentation and protection of information will be discussed as well as segregating of task lists. A clear demarcation in duties allows additive effects to be realized as the project evolves and helps reduce or eliminate delays. Projects will fail when effective communication channels are not in place. Methods for aligning resources to tasks must be tracked and progress assessed at frequent intervals. An early appreciation for true and accurate complexity of the task is critical to avoid over-resourcing and cause project delays. A major component of implementing a CUAS Program is deterrence. A healthy CUAS Program communicates its presence to help educate UAS operators who may be careless or clueless about flight regulations or restrictions. Messages about potential impacts to their drone, fines and penalties is usually enough to deter curious operators from flying into restricted areas. UAS operators engaging in criminal activity will not usually respond to any form of deterrence. These individuals should be considered a more determined malefactor and met with a rapid and coordinated response to neutralize and disrupt the unauthorized UAS activity. This presentation will provide successful concepts and strategies used to deploy an effective and efficient CUAS Program at a high-security nuclear facility in a rapid, safe and secure manner.

State

United States

Gender

Male

Primary author: Mr ATENCIO, Julian (Los Alamos National Laboratory)

Presenter: Mr ATENCIO, Julian (Los Alamos National Laboratory)
Track Classification: PP: Nuclear security of nuclear fuel cycle facilities: emerging technologies and associated challenges and complex threats
The Application of the Graded Approach to Physical Protection of Radioactive Sources in the United States

Development and oversight of security measures that account for the overall risk posed by radioactive materials requires integration of safety and security programs. Implementing a graded approach to security allows the U.S. Nuclear Regulatory Commission (NRC), along with our Agreement State partners, to ensure adequate protection without unnecessary burden. This allows the United States (US) to realize and take full advantage of the benefits of the various uses of radioactive materials. The NRC will present on its efforts to utilize a graded approach in the establishment of a strong regulatory framework to ensure the safety, security, and control of radioactive sources – from allowing exemptions from regulations for specific items, through sources and uses for which prudent management practices or existing safety requirements are sufficient, to the highest activity sources and practices that deserve the tightest control.

The US framework relies on various safety and security analyses, including threat, vulnerability, and consequence, to determine the appropriate framework and requirements for each circumstance. These analyses form the basis for the graded security for all civilian radioactive and nuclear material in the U.S. For example, sources that present minimal to negligible hazard, such as smoke detectors and gunsights, are exempt from licensing entirely for the end-user, while still other sources, such as those in robust devices, are subject to registration and notifications of transfers to the regulatory agency. For the majority of licensed civilian radioactive and nuclear material in the U.S. the physical protection measures can be found in 10 CFR Part 20, in paragraphs 1801 and 1802. Although, in short, these paragraphs state only that licensees must secure their material while in storage and that it must be under constant surveillance while in use – they do not specify exactly what means a licensee must use to accomplish those objectives. Thus, licensees must develop processes and procedures that are subject to inspection, to meet these objectives.

For other licensed material, and for specific modalities of use, additional (not replacement) requirements apply. An example of this is a well logging licensee who possesses a category 3 americium-241/beryllium source. This licensee must comply with the security requirements in 10 CFR Part 20, but also must comply with the additional requirements in 10 CFR Part 39 that are specific to well logging operations and, among other things, include prescriptive requirements for source control and security.

For sources or aggregated quantities of radioactive material that the U.S. has determined to be risk-significant, that is that meet or exceed the category 2 threshold, further requirements of 10 CFR Part 37 must be implemented by the licensee to ensure additional physical protection. An example of this situation is an industrial radiography licensee who possesses a camera (or multiple cameras) containing a category 2 iridium-192 source who must comply with 10 CFR Part 20, the additional specific safety requirements for radiography in 10 CFR Part 34 such as personnel wearing alarming dosimetry, and further security requirements in 10 CFR Part 37 such as providing extra barriers for their mobile source(s). These examples demonstrate the commitment to maintaining adequate protection of workers, the public, the environment, and the security of the U.S., but also demonstrate a recognition of the differences among the large population of users of radioactive and nuclear material within the U.S.

The NRC has conducted multiple efforts to evaluate this framework in the past 3 years, has made revisions to further enhance its source protection program, and continues to monitor the threat environment to proactively identify any need for changes to ensure the security of these materials from potential terrorist threats. This paper will present this graded approach to the integrated safety and security framework that the NRC and Agreement States utilize, expanding on specific examples of this application, and will briefly describe efforts to evaluate and enhance this approach.
over the years.

State
United States

Gender
Female

Primary author: CERVERA, Margaret (United States Nuclear Regulatory Commission)
Presenter: CERVERA, Margaret (United States Nuclear Regulatory Commission)

Track Classification: PP: Risk-informed approach to the security of radioactive material in use and in storage
Using a Graded Approach in the Oversite of Security at NRC-Licensed Research Reactors

Monday, 10 February 2020 17:15 (15 minutes)

The NRC licenses and provides oversight of the civilian use of special nuclear materials (SNM) used at research reactors. Regulatory oversight seeks to protect public health and safety, promote the common defense and security, and protect the environment.

The existing SNM physical protection regulatory requirements at research reactors are graded using a material categorization approach similar to that found in “Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Materials” (INFCIRC/225/Revision5). The application of a graded approach is essential given the wide diversity among the regulated community of research reactors. The NRC regulates 31 research reactors, some are located on federal government campuses, some are privately owned, but most are located at universities. While some of the university research reactors are located off campus in remote locations, many are in classroom buildings in the middle of campus.

The regulations identify requirements for physical protection of SNM, depending on its Category, using a defense is depth approach. The ease of separability of SNM from other radioactive materials and external radiation levels is also considered to a varying degree in assigning different physical protection requirements or in exempting certain materials from physical protection requirements. Finally, security requirements are applied based on power level, with research reactors of higher power level requiring additional measures to protect against sabotage.

This presentation will discuss the NRC regulatory framework as it applies to research reactors and their unique environments. It will also show how the NRC applies security requirements on a site-specific basis using a graded approach. The presentation will also discuss lessons learned and effective practices identified regarding the implementation of regulations and interagency initiatives as they apply to research reactors. Some of which were highlighted in 2013 when the NRC hosted an International Physical Protection Advisory Service Mission (IPPAS).

State

United States

Gender

Female

Primary author:  Ms REED, Elizabeth (U.S. NRC)

Presenter:  Ms REED, Elizabeth (U.S. NRC)

Session Classification:  Research Reactor Security

Track Classification:  PP: Research reactor security
UGANDA’S CAPABILITIES AND CHALLENGES ON PREVENTION AND DETECTION OF NUCLEAR AND RADIOACTIVE MATERIAL

UGANDA’S CAPABILITIES AND CHALLENGES ON PREVENTION AND DETECTION OF NUCLEAR AND RADIOACTIVE MATERIAL.

MR. OBOO MOSES
Radiation Protection Officer, Atomic Energy Council
Plot 29/33 Kampala Road, P.O. BOX 7044
Kampala, Uganda

Prevention and detection of radioactive sources plays a major role in helping to mitigate the incidences of malicious acts or sabotage of facilities with radioactive sources.

The Atomic Energy Council (AEC), the national regulatory body of Uganda has aided the implementation of the prevention and detection mechanisms in facilities having radioactive sources through regulatory inspections, installation of security detection systems at Uganda Cancer Institute - radiotherapy department and at the Temporary Waste Storage Facility owned by AEC, Training of personnel from Uganda Police-Counter Terrorism department, Customs officers and other security agencies in the country, development of two safety guides namely guide on security of high category radioactive sources, and the guide on physical protection systems and measures for facilities housing radioactive sources. These were developed to guide the authorized persons on what they are expected to put in place and also helped AEC to develop an inspection checklist on security requirements and recommendations.

The country currently has three radiation porter monitors installed at the major designated points of entry, there are joint security and intelligence operations at the border points, and there are communication mechanisms for responding to information and instrument alarms and generally there is government political will to support the program of having radiation detection systems at various agencies responsible for nuclear security.

Currently the country doesn’t have radiation portal monitors at all the major border points to the country, the regulatory body lacks equipment to carry out food and water testing on the level of radionuclide contained in them, there are no installed detection systems at the metal recycling industries. There is limited detection at annual Major Public Events in the country e.g. the Uganda Martyrs day Celebrations, National prayer day among others.

This paper will discuss broadly on the current capabilities and the challenges faced by the regulatory body and other agencies in ensuring effective implementation on having prevention and detection systems at various strategic locations in the country and also suggest the key recommendations to government and various stakeholders especially Uganda Revenue Authority-Customs department and Uganda Police Force on how to improve on the prevention and detection systems already in place.

Addressing the above mentioned challenges will improve on the prevention and detection systems for radioactive sources in Uganda. It should also be noted that the Ugandan government, the IAEA and the various stakeholders will have a role to play in ensuring that this will come to effect.

State

Uganda
Gender

Male

Primary author:  OBOO, MOSES
Presenter:  OBOO, MOSES

Track Classification:  MORC: Building and maintaining nuclear security detection architecture
Crediting Law Enforcement Response in the U.S.
Nuclear Regulatory Commission’s Security Inspection Program

Following Commission direction, the U.S. Nuclear Regulatory Commission’s (NRC) staff has recommended ways to credit a broader set of operator actions, including the use of Diverse and Flexible Mitigation Capability (FLEX) equipment, and credit response by local, State, and Federal law enforcement in the NRC’s security inspection program. This paper describes the NRC staff’s recommendation for crediting law enforcement response, how the recommendation was developed, and next steps to evaluate future implementation of that credit by NRC’s licensed nuclear power reactors.

The NRC staff is evaluating providing credit to licensees for law enforcement response by establishing a security bounding time, which is defined as the elapsed time, measured from recognition of an attack, required for the licensee to preclude adversary interference sufficiently to allow performance of operator actions that can prevent or mitigate radiological sabotage. NRC’s power reactor licensees are required to establish, maintain, and implement a physical protection program that is designed to protect against the design basis threat (DBT) of radiological sabotage. By establishing a security bounding time, and crediting law enforcement response, a licensee could add operator actions and components, including FLEX equipment, to target sets and potentially revise their protective strategies.

The NRC staff sought external stakeholder views during public meetings on November 13, 2018, and December 17, 2018. At these meetings, the staff presented ideas for providing credit for operator actions, FLEX, and for law enforcement response. Industry stakeholders voiced multiple views regarding whether they would seek credit for law enforcement support within the protected area. Many licensees indicated that law enforcement could reasonably be expected to assist in neutralizing adversaries in the owner controlled area, based on the recognition that in an actual emergency, State and local government officials will exercise their best efforts to protect the health and safety of the public. The Nuclear Energy Institute (NEI) presented a proposal for security bounding time, which was subsequently provided in a white paper, “Determination of a Site-specific Security Bounding Time,” dated January 10, 2019 (ADAMS Accession No. ML19010A373).

The NRC staff is engaging with stakeholders to fully evaluate the process that a licensee would follow to receive some credit for law enforcement tactical support through the determination of a security bounding time. Specifically, the licensee would (1) adopt a default security bounding time that would be set by the NRC or develop a shorter, site-specific security bounding time using an approved methodology; (2) use the security bounding time to determine the allowable credit for a tactical response by a law enforcement agency (i.e., in the development of target sets); and (3) consider this credited response in the design and evaluation of the licensee’s physical protection program (i.e., in the development of the protective strategy).

State

United States

Gender

Female
Primary author: Mr SULLIVAN, Frederick (U.S. NRC)

Co-author: HELTON, Shana

Presenter: HELTON, Shana

Track Classification: CC: National nuclear security regulations
Cesium Chloride: Risks and Alternatives

Recommendation 3.19 of the IAEA Nuclear Security Series No.14, Nuclear Security Recommendations on Radioactive Material and Associated Facilities states, "The State should assess the potential threats, the potential consequences and the likelihood of malicious acts, and then develop a legislative and regulatory framework that provides for efficient and effective security measures to address the threat." Malevolent use of radiological material and the risk associated with it is represented by the likelihood of an attack and the consequence associated with that attack. The U.S. National Academy of Sciences used a risk-based analysis for its 2008 Radiation Source Use and Replacement Study, one of the early reports that used a risk model to assess the potential malevolent use of radiological materials, specifically a radiological dispersal device (RDD), and recommend solutions to reduce the risk, such as phasing out the use of cesium chloride (CsCl). The United States Department of Energy National Nuclear Security Agency’s Office of Radiological Security has a worldwide program to expand and accelerate efforts to reduce the potential malevolent use of CsCl, referred to as the Global Cesium Security Initiative (GCSI). GCSI works either to improve radiological material security at facilities with the goal of achieving material containment in coordination with enhanced delay through in-device delay technologies and law enforcement response integration or to achieve permanent risk reduction through replacement of CsCl with alternative technologies.

This presentation will review the analyses and real-world accidents that illustrate the unique national security risks associated with CsCl. Applications and uses of CsCl devices will be discussed with an assessment showing the global footprint of these devices. Alternative non-radioisotope technologies will be discussed along with the incentives and barriers for using these alternatives. GCSI’s approach to and successes of collaborating with international partners that use CsCl-based devices to provide advanced security enhancements, assistance to replace CsCl devices with alternative technologies, and support for removal or consolidation of disused CsCl devices will be highlighted.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy’s National Nuclear Security Administration under contract DE-NA0003525.

State
United States

Gender

Primary author: Dr EKMAN, Mark (Sandia National Laboratories)
Co-authors: Dr LADD, Mark (Sandia National Laboratories); Dr SOLODOV, Alexander (Sandia National Laboratories)
Presenter: Dr EKMAN, Mark (Sandia National Laboratories)
Track Classification: CC: Innovative technologies to reduce nuclear security risks and improve cost effectiveness, where feasible
Risk-Informing Nuclear Security Regulatory Approaches

The U.S. Nuclear Regulatory Commission (NRC) has increased its efforts to risk inform security regulatory approaches. This paper will highlight some of the ongoing activities as well as lessons learned. The goal of the NRC’s initiative to risk-inform security is to ensure the staff is applying the appropriate level of regulation and establish requirements for security that are commensurate with the risk of the activity and material to be protected. It also provides an opportunity to add realism to the program including the use of real-world data during the development of force-on-force exercise scenarios. Assessing risk in security has similarities, as well as differences, to assessing risk in the safety world. One particular difference is the initiating event for safety scenarios is typically a random event allowing for the actual calculation of risk. However, the initiating event for security scenarios is not a random occurrence since an adversary (as defined by the design basis threat) initiates an attack which makes it more of a challenge to calculate risk. This paper will present some of the ways this concept has been applied to risk analysis for a physical security program and how the NRC has accounted for this difference.

Risk informing initiatives are important activities for the U.S. Nuclear Regulatory Commission. The NRC has begun risk informing several ongoing security activities including the use of current threat assessment information to inform the development of force-on-force exercise scenarios, the use of site-specific threat conditions to determine appropriate implementing timelines for security compensatory measures and revising the baseline security inspection program to ensure the appropriate level of oversight based on reasonable assurance of protection. In addition to the work the NRC has done, NRC licensees have also undertaken efforts to utilize risk information in their security activities and their interest continues to grow, with a stated goal of increasing efficiency while maintaining safety and security. One major activity that has been underway for several years is the use of modeling and simulation software to conduct vulnerability assessments (computer modeling) of licensed facilities. In many ways, these assessments have many similarities to probabilistic risk assessments conducted in the safety arena. Risk informed security will continue to play an increasing role in the NRC’s regulatory approaches.

State

United States

Gender

Male

Primary author:  Mr HUYCK, Doug (U.S. NRC)

Presenter:  Mr HUYCK, Doug (U.S. NRC)

Track Classification:  PP: Physical protection systems: evaluation and assessment
Development and Maintenance of the Design Basis Threat for Civilian Nuclear Facilities in the United States

Establishing a design basis threat (DBT) provides an effective means through which a regulatory body can communicate risk-informed performance-based security standards to its operators and licensees. In the United States, the U.S. Nuclear Regulatory Commission (NRC) is responsible for regulating the physical protection of civilian nuclear material and facilities. The NRC maintains two design basis threats: one to address radiological sabotage that is applicable to power reactors and fuel cycle facilities, and a second DBT for theft or diversion of nuclear material that is applicable to fuel cycle facilities.

The NRC first issued DBTs in the late 1970s. Following the terrorist attacks on September 11, 2001, the NRC undertook a thorough review of its security regulations. This review included an evaluation of the adequacy of the agency’s existing DBTs against the agency’s analysis of the threat environment. As a result of its review, the agency made revisions to its DBTs first in 2003 and again in 2007.

The NRC maintains its DBTs through a review process called the Adversary Characteristics Screening Process. The agency revised the process as a result of lessons learned through its 2003 and 2007 reviews of the DBT. The Adversary Characteristics Screening Process consists of steps that NRC staff follow in determining whether to recommend a change to the DBT. These steps ensure that input from regulatory, intelligence, law enforcement, and stakeholders is considered when the agency considers a revision to a DBT. Though developed independently, this process has many aspects in common with the process outlined in IAEA Nuclear Security Series No. 10, "Development, Use and Maintenance of the Design Basis Threat."

The NRC established the Principles of Good Regulation to guide the agency in its regulatory activities: independence, openness, efficiency, clarity, and reliability. The DBTs communicate the performance-based requirements for physical protection of power reactors and fuel cycle facilities is an effective means of regulating nuclear security while adhering to those principles.

State

United States

Gender

Male

Primary authors:  Mr YIP, Brian (U.S. NRC); Mr WHITNEY, James (U.S. NRC)

Presenter:  Mr YIP, Brian (U.S. NRC)

Track Classification:  PP: Design basis threat and threat assessment: prevention and protection
U.S. Cyber Security Experiences

The increasing advancement of digital technology and the large amount of digital equipment in nuclear power plants have created new cyber threats to the nuclear power industry. In the U.S., nuclear power plants have implemented measures to address ever increasing cyber threats since the September 11, 2001 terrorist attacks. The NRC published a cyber security rule for power reactor licensees (10 CFR 73.54) in 2009.

The power reactor licensees implemented the cyber security rule at their facilities (cyber security program) in two steps. The first step had seven milestones, referred to as “interim milestones”. The licensees implemented security measures that would address significant threat vectors so that nuclear power plants were protected. The licensees completed the implementation of these security measures by 2012. The NRC inspected licensees’ implementation of the interim milestones between 2013 and 2015. The second step involves full implementation of the cyber security program. In general, licensees fully implemented the cyber security program at their facilities by 2017. The NRC began inspecting licensees’ full implementation program in July 2017 and this inspection is scheduled to be completed in 2020. The NRC performs a two-week onsite inspection. As of December 2018, the NRC completed the inspections of 20 sites.

The NRC has gained valuable insights on implementing cyber security programs at commercial nuclear power plants in the United States. This paper provides an overview of the challenges faced in implementing a cyber security oversight program for nuclear power plants, as well as the lessons learned from its implementation. In addition, this paper will also discuss those controls that are effective in minimizing the cyber attack surfaces for the commercial nuclear power plants in the U.S.

State
United States

Gender
Male

Primary author: Mr BEARDSLEY, James (U.S. NRC)
Presenter: Mr BEARDSLEY, James (U.S. NRC)

Track Classification: CC: Information and computer security considerations for nuclear security
Nuclear Regulatory Authority Activities in Nuclear Security

Undoubtedly nuclear security has surfaced as a subject of concern on the international agenda and has gained attention at the highest political level in several States. Argentina has demonstrated its strong commitment towards it and has recognized the unique role of the IAEA in strengthening global nuclear security. Argentina has also come to the conclusion that a number of stakeholders must be taken into account in order to define general requirements and necessary control standards.

At the regulatory level, the Nuclear Regulatory Authority (ARN) of Argentina is mandated by the Nuclear Activity National Act to carry out tasks with the objective of preventing the commission of intentional acts that may lead to severe radiological consequences or unauthorized withdrawal of nuclear material or other materials or equipment subject to regulation and control. It has federal competence to regulate the nuclear activity on physical protection and also on transport of radioactive materials, radiation and nuclear safety and non-proliferation.

ARN dictates regulatory standards, issues the permissions and licenses authorizing practices and installations, controls the compliance with standards, requirements and license conditions, enforces this compliance and has a leading role in the preparation and response to radiological and nuclear emergencies. It is worth highlighting that it is an autonomous body reporting to the country’s Presidency, and is independent of any organization dedicated to the use or the promotion of nuclear energy in any of its forms.

Regarding physical protection, ARN is the competent authority responsible for the implementation of the regulatory functions on the physical protection of nuclear material and facilities and the security of radioactive sources, and therefore has a key role in complying with the Convention on the Physical Protection of Nuclear Material and its Amendment (CPPNM, the single legally binding instrument on the matter).

The paper will describe and provide an update on the activities performed by ARN in the field of nuclear security between the 2016 and 2020 Ministerial International Conferences. It is worth noting that the chosen period includes a key development: the entry into force of the CPPNM Amendment.

The mentioned activities will be described in detail under three topics: the Argentine regulatory framework, capacity building, and international cooperation. The first one will summarize the ARN’s education and training activities in nuclear security and the efforts made to enhance the nuclear security culture. The second area will deal with the process to adapt and adequate Argentine physical protection standards (in terms of normative, requirements and license conditions) to the current international legal instruments. Finally, the third part will cover cooperation activities at the regional and international level.

State
Argentina

Gender
Female
Primary authors: ROSTON, Maria Victoria (Nuclear Regulatory Authority of Argentina); Ms ACOSTA, Gabriela (Nuclear Regulatory Authority); Mr TAPIA, Matias (Nuclear Regulatory Authority); Mr ZUNINO, Pablo (Nuclear Regulatory Authority)

Presenter: ROSTON, Maria Victoria (Nuclear Regulatory Authority of Argentina)

Track Classification: CC: National nuclear security regulations
Physical Protection of Nuclear Materials During Transport

The Nuclear Regulatory Authority (ARN) was established as an autonomous body reporting to the Presidency of Argentina by Act 24804 (known as the Nuclear Activity National Act), which came into force in 1997, and is empowered to regulate and control the nuclear activity in Argentina. Its objective is to establish, develop and enforce a regulatory system applicable to all nuclear activities carried out in the country.

In its capacity as the national authority on all issues concerning radiation and nuclear safety, non-proliferation assurances, physical protection and transport of radioactive materials, the ARN grants licenses, authorizations and permits, as appropriate, in connection with facilities, practices and personnel associated with radioactive materials. Additionally, the ARN performs control activities to ensure that persons responsible for each practice comply with the provisions set forth in the standards and other regulatory documents.

Regarding the physical protection against robbery, removal or unauthorized use of nuclear materials, and sabotage against nuclear facilities, the ARN requires the Responsible Entity to implement a complete physical protection system applicable to nuclear facilities and materials in accordance with the regulatory requirements set forth by the ARN.

The establishment of regulatory criteria concerning the security of radioactive materials other than nuclear materials is also addressed by ARN, through the development of a policy which is reinforced by the reasonable assessment of the risks in this area that are relevant to the Argentine context.

The transport of nuclear and other radioactive materials is considered one of the most risky stages of materials' life since they are more vulnerable being out of the fences of a facility. In this sense, there are two different groups of measures and procedures to protect them during transport.

Regarding the safety during transport of radioactive material, all international, regional and national organizations responsible for regulation of land, air, river and sea transport of hazardous materials have endorsed the safety requirements contained in the provisions of the IAEA SSR-6 “Regulations for the Safe Transport of Radioactive Material”, 2012 Edition (currently, the 2018 Edition is available). The transport of nuclear and other radioactive material within Argentina shall be carried out in accordance with standard AR 10.16.1 relating to “Transport of Radioactive Materials”, the text of which is identical to the aforesaid IAEA Regulations.

On the other hand, the security aspects during transport of nuclear materials are considered in standard AR 10.13.1 "Standard of Physical Protection of Nuclear Materials and Facilities”. This regulation states that levels, procedures and recommendations for the physical protection of materials protected during international transport shall be in accordance with Annexes I and II of the Convention on the Physical Protection of Nuclear Material (CPPNM).

In this paper we will approach the differences between physical protection of nuclear material and nuclear security of other radioactive materials during transport, from the regulatory point of view, and the challenges that this distinction poses to international regulations.

State

Argentina

Gender
Female

**Primary authors:** ROSTON, Maria Victoria (Nuclear Regulatory Authority of Argentina); Mr ELECHOSA, Christian (Nuclear Regulatory Authority)

**Presenter:** ROSTON, Maria Victoria (Nuclear Regulatory Authority of Argentina)

**Track Classification:** PP: Transport of nuclear and other radioactive material: practices, challenges and regulatory issues
Preparing for a nuclear terrorist attack by creating a unified response through national nuclear response frameworks

Abstract: As attempts by terrorists to obtain nuclear and radiological weapons and materials increases, it is important to plan and prepare for terrorists detonating an R/N bomb. A key preparation component is a national nuclear response framework (NNRF), which details the policies, procedures, capabilities, and priorities for responding to a nuclear terrorist attack. Defining the roles and responsibilities as well as coordination mechanisms among national and international bodies will help ensure the framework creates a unified response. In turn, a unified response will help streamline the response and avoid confusion in the field. The paper will detail three important coordination factors within a NNRF: interagency coordination; international coordination; and public communications. The Global Initiative to Combat Nuclear Terrorism identified these key national nuclear framework components during a Nigerian hosted workshop focused on adapting all-hazards response frameworks to nuclear response frameworks.

Discussion at the workshop highlighted a number of key best practices related to NNRFs. A NNRF should take a multi-faceted approach to detailing agencies’ roles and responsibilities. Frameworks clearly define the roles of each agency. For instance, first responders should know their in-field roles and priorities in advance of an attack. Additionally, the frameworks outline interagency coordination. Each responsibility denotes a lead agency as well as defined supporting agencies. A country also identifies an agency to lead the overall response. Countries can hold interagency exercises as way to ensure all agencies understand how to operate and coordinate based on their NNRF. Agencies should not only prepare with communicating with each other but also with the public.

The workshop also focused on crisis communications pertaining to public messaging. Countries should outline a public messaging strategy in preparation of an attack in order to deliver a unified public message. A unified message will ensure there is no conflicting information disseminated and manage public risk perception. Key preparation factor is identifying messaging priorities and a lead authority to communicate information to the public. To ease messaging during a response, agencies can coordinate to create pre-approved messaging for the lead public messaging authority to disseminate during an attack. It is important to not only prepare nationally but also internationally.

Participants at the Nigerian workshop stressed the importance of international coordination and communication. NNRFs should address international requirements, protocols, and coordination mechanisms to ensure the attacked nation receives the highest amount of aid possible and safeguard other countries. Effective bilateral coordination requires both strong relationships between institutions in each country and established formal mechanisms for exchanging information. Agencies can formalize information sharing and coordination through protocols and agreements. Nations should also consider plans and protocols for submitting assistance requests to international organizations and regional partners. Furthermore, nations should understand the relevant international legal instruments they are party to and detail the procedures needed to comply with those agreements. Through bilateral and multilateral exercises, countries can test these international protocols and coordination procedure.

State
Nigeria

Gender

Male

Primary authors: Mr IBRAHIM, Abdulmajeed (Nigerian Nuclear Regulatory Authority); Dr ISA, Sambo (Nigerian Nuclear Regulatory Authority); Prof. DIM, Lawrence (Center for Energy Research Development and Training)

Presenters: Mr IBRAHIM, Abdulmajeed (Nigerian Nuclear Regulatory Authority); Prof. DIM, Lawrence (Center for Energy Research Development and Training)

Track Classification: CC: Emergency preparedness and response and nuclear security interfaces
Responding to the Detection of Special Fissionable Materials and Other Threat Materials with Case Studies

This paper will discuss the challenges posed in confidently adjudicating alarms when nuclear materials or other potential threat materials are detected in secondary inspection. Primary radiation detection systems are installed at three seaports in Spain. Each of these seaports have a spectroscopic portal monitor (SPM) that is used for secondary inspection. Two additional seaports in Spain have spectroscopic portal monitors installed to inspect cargo. The vast majority of primary alarms that are sent to secondary inspection result in the confirmation of naturally occurring radioactive materials (NORM) as declared on the manifest. However, a small fraction (approximately five percent) of the alarms generated on the SPM are threat alarms indicating the potential presence of radioactive industrial, medical or nuclear material isotopes. Responding to the detection of special fissionable material in secondary inspection presents unique challenges that must be addressed to provide an acceptable degree of confidence that nuclear materials are not being smuggled. These challenges are exacerbated when special fissionable material is potentially detected in land/sea cargo containers. A number of cases studies from Spain will be presented that illustrate the technical obstacles and other challenges encountered.

Challenges
1. Land/sea cargo containers have the potential to contain large amounts of densely packed NORM materials emitting relatively high levels of radiation that can make use of sodium iodide radiisotope identification detectors in the spectrometric portal monitors problematic requiring the use of high purity geranium detectors to exclude the presence of threat materials.
2. Analysis of complex spectra require a degree of training that is not readily provided to the vast majority of spectrometrists in the world as most spectrometrists are trained to analyze spectra related to the nuclear fuel cycle or other industries using radioactive materials.
3. Development of technical procedures for use by front line officers to collect the data needed for remote expert support teams to analyze and properly adjudicate alarms.
4. Providing dedicated 24/7 support to front line officers from expert support team members to provide primary/secondary alarm data analysis to determine if cargo containers need to be detained for tertiary inspection.
5. Social issues surrounding the potential detection of special fissionable materials and the need to control information.
6. Returning containers containing industrial/medical material out of regulatory control (MORC) to the country of origin.

State
United States

Gender
Not Specified
Primary authors:  Mr GILLISPIE, Obie (Los Alamos National Laboratory);  Mr ANGEL DE LA RUBIA RODIZ, Miguel (Estatal de Administracion Tributaria)

Presenter:  Mr GILLISPIE, Obie (Los Alamos National Laboratory)

Track Classification:  MORC: Preventing illicit trafficking of nuclear and radioactive material
The Border Monitoring Working Group Front Line Officer Training

The Border Monitoring Working Group (BMWG) was established in 2005 by the IAEA, the European Union (EU) and the United States (U.S.) to promote coordination between its members and to serve as a forum for discussion and exchange of information on plans and programs to be implemented by its members in cooperation with the recipient countries to combat the illicit trafficking of nuclear and other radioactive material out of regulatory control. Since its establishment, the BMWG has proven to not only be an effective tool for avoiding duplication and maximizing and targeting resources, but also a forum to address common technical concerns and jointly develop capacity building tools. One such example of a capacity building tool that has been jointly developed and implemented is BMWG Frontline Officer Training Course on Nuclear Security Detection. This course trains frontline officers with radiation detection duties, such as police, border guard, customs officers, and gendarmerie in areas including radiation awareness, nuclear security threat awareness, radiation detection equipment operation, alarm adjudication, and secondary inspection techniques among other things. This paper will focus on the design and historical implementation of this course as well as introduce recent updates that reflect advances in adult learning principles. In addition, the implementation of this course at select nuclear security support centers will also be presented.

State
Germany

Gender
Male

Primary author:  Dr GALY, Jean (European Commission, Joint Research Centre)
Co-authors:  Mr VAN-HEESWIJK, Wilhelmus (European Commission, DG Taxation and Customs Union); Dr PEPER, Shane (U.S. Department of Energy, Pacific Northwest National Laboratory)
Presenter:  Dr GALY, Jean (European Commission, Joint Research Centre)

Track Classification:  CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
Conversion of Miniature Neutron Source Reactors from High Enriched Uranium to Low Enriched Uranium

International work to convert or decommission highly enriched uranium (HEU) research and test reactors to low enriched uranium (LEU) fuel has taken place since 1978. The decades-long effort is achieved by a multilateral group of stakeholders with the objective of reducing and eventually eliminating the civilian use of HEU.

The Reduced Enrichment for Research and Test Reactors (RERTR) Program currently operated by DOE/NNSA Material Management and Minimization (M3) Conversion Program, exists to address this objective. Additionally, the Miniature Neutron Source Reactor (MNSR) community joined with the International Atomic Energy Agency (IAEA) to further this international objective by launching an IAEA-coordinated research project (CRP) to coordinate global activities to convert MNSRs to LEU in 2006.

MNSRs are low power (nominal 30 kW) research reactors designed and manufactured by the China Institute of Atomic Energy (CIAE). MNSRs are mainly used for neutron activation analysis, training, and testing of nuclear instrumentation. The first MNSR, the Prototype at the CIAE facility in Beijing, was put into operation in 1984. Eight other MNSRs were built in China and other countries and fuelled with HEU (~ 90%), with a design slightly different from the Prototype.

As a result of the IAEA CRP, a viable design was found to convert the MNSRs from their original HEU fuel enriched to 90 wt% uranium-235 to an LEU fuel enriched to 13 wt% uranium-235 with no degradation in overall reactor performance. Representatives from each country with an MNSR participated in the CRP, along with representatives from the U.S. Department of Energy (DOE) and the U.S. national laboratories. At the conclusion of the CRP in 2010, it was decided to establish an MNSR Working Group among MNSR operators, designers, and stakeholders to continue the work of the CRP.

The primary objective of the working group is to coordinate activities related to the conversion of MNSRs to LEU and the return of the HEU to China. Since the successful conclusion of this CRP and establishment of the Working Group, there have been three successful conversions of MNSRs from HEU fuel to LEU fuel – the prototype at the CIAE, the Ghana Research Reactor 1 (GHARR-1), and the Nigeria Research Reactor 1 (NIRR-1).

In contrast with decades of previous conversion projects in the RERTR program which have been managed on a largely bilateral basis, the MNSR conversion projects have been noteworthy for their reliance on multiple international stakeholders. The multilateral nature of the conversion projects, as well as the completion of three conversions in three years, have allowed for the iterative development and clarification of the multilateral process for planning and implementing these conversion projects. The success of these projects is defined by multilateral cooperation on conversion feasibility analysis, early definition of regulatory and bureaucratic procedures, and frequent, regular communication among stakeholders.

State

United States

Gender
Not Specified

**Primary author:** Ms DICKERSON, Jaci (DOE/NNSA)

**Presenter:** Ms DICKERSON, Jaci (DOE/NNSA)

**Track Classification:** PP: Minimization, on a voluntary basis, of high enriched uranium within civilian stocks and where technically and economically feasible
Ensuring a Stable Supply of Mo-99 in the U.S. without the use of HEU

Monday, 10 February 2020 15:15 (15 minutes)

Ensuring a Stable Supply of Mo-99 in the U.S. without the use of HEU

Technetium-99m (Tc-99m) is a radioisotope used in approximately 80% of all medical imaging procedures across the globe. With a half-life of approximately six hours, this important medical radioisotope cannot be stockpiled and must be either used immediately upon direct production or repeatedly milked from generators bearing the parent isotope, molybdenum-99 (Mo-99), which has a half-life of approximately 66 hours. Historically, Mo-99 has been produced in research reactors by the irradiation of targets bearing highly-enriched uranium (HEU) followed by chemical separation and purification. In order to minimize the proliferation risks posed by medical isotope production, the U.S. National Nuclear Security Agency (NNSA) has funded a multi-year program to accelerate the deployment of technologies to produce Mo-99 without the use of HEU. Internationally, this work has focused on replacing HEU targets with low-enriched uranium (LEU) equivalents. Within the U.S., operating under a full cost-recovery paradigm, NNSA has directly funded the research and development of accelerator-based technologies and reactor target-based technologies via cost-sharing Cooperative Agreements with potential commercial producers.

One of the Cooperative Agreement partners, NorthStar Medical Radioisotopes (NorthStar), is pursuing a dual production pathway for Mo-99: irradiation of enriched Mo-98 targets in the University of Missouri Research Reactor (MURR) and electron beam accelerator-based production using Mo-100 targets at their production site in Wisconsin. NorthStar’s production method supplants the traditional generator-based supply chain by use of the NorthStar RadioGenix system in radiopharmacies.

Another Cooperative Agreement partner, SHINE Medical Technologies (SHINE), uses a deuteron beam accelerator and tritium gas target to produce high-energy neutrons. These neutrons are thermalized and multiplied before irradiation of a liquid LEU target solution in a subcritical configuration. After each production cycle, the Mo-99 is extracted from the LEU solution, which is reconditioned and recycled to minimize total uranium usage. The SHINE production method is designed to be compatible with the existing Tc-99m generator manufacturer supply chain.

The third Cooperative Agreement partner, NorthWest Medical Isotopes (NWMI), produces Mo-99 using LEU solid targets that are able to be irradiated in multiple research reactors and shipped to their target processing facility in Missouri for dissolution and Mo-99 extraction and purification. Like SHINE Medical Technologies, the NWMI production method is designed to be compatible with the existing Tc-99m generator manufacturer supply chain.

The fourth Cooperative Agreement partner, Niowave Inc. (Niowave), uses a superconducting electron linear accelerator to irradiate a neutron-generating target surrounded by LEU production targets. After each production cycle, the targets are dissolved and Mo-99 is extracted and purified. Like SHINE and NWMI, the Mo-99 produced by Niowave is designed to be compatible with the existing Tc-99m generator manufacturer supply chain.

The organization also provides technical support by making resources from the U.S. Department of Energy National Laboratories available to potential commercial producers. In addition to the Cooperative Agreement partners, U.S. National Laboratory assistance has been provided to both international producers and U.S. potential producers who have not been directly-funded by NNSA. An overview of the U.S. National Laboratory technical support will also be given.
**State**

United States

**Gender**

Not Specified

**Primary author:** Dr HELTEMES, Thad (Argonne National Laboratory)

**Presenter:** Dr HELTEMES, Thad (Argonne National Laboratory)

**Session Classification:** Innovative technologies to reduce nuclear security risks and improve cost effectiveness, where feasible

**Track Classification:** CC: Innovative technologies to reduce nuclear security risks and improve cost effectiveness, where feasible
Strengthening Testing and Evaluation Capabilities for the Long-Term Sustainability of Nuclear Detection Architectures

R. Dietrich1, J. Erchinger2, Y. Han3, J Hoyt4, P. Kolbas4, J. Liang5, L. Qian 6, and J. Shergur7

1 Sandia National Laboratories, P.O. Box 5800, Albuquerque, NM 87185 USA
2 Los Alamos National Laboratory, P.O. Box 1663, Los Alamos, NM 87545 USA
3 China State Nuclear Security Technology Center, No. 67 Fusheng Ave., Fangshan District, Beijing, China
4 Pacific Northwest National Laboratory, P.O. Box 999, Richland, WA 99352 USA
5 China National Institute for Metrology, No. 18 North 3rd Ring Road, E., Chaoyang District, Beijing, China
6 General Administration of China Customs, No. 6 Jianguomennei Ave., Beijing, China
7 Oak Ridge National Laboratory, 1 Bethel Valley Rd, Oak Ridge, TN 37830 USA

E-mail of the corresponding author: joel.hoyt@pnnl.gov

The US Department of Energy (DOE) National Nuclear Security Administration’s Office of Nuclear Smuggling Detection and Deterrence (NSDD formerly referred to as Second Line of Defense and Megaports) has worked with more than sixty countries to build, strengthen, and sustain capabilities that enable deterrence, detection, and investigation of the illicit trafficking of nuclear and radioactive materials. A central element of these capabilities is effective radiation detection equipment, including radiation portal monitors and handheld radiation detection devices. For this equipment to successfully serve the nuclear security regime, it is critical the equipment is selected based upon mission-driven radiation detection/identification, environmental robustness, and operational requirements, and rigorously tested to ensure its compliance with each. While requirements development and subsequent testing and evaluation is a central focus when acquiring new or replacement equipment, the capability is also part of a sustainable equipment life-cycle program that empowers the nuclear security regime to evaluate the impacts from changes to technology, operational protocol, or the operational environment.

Beginning in 2015, the US DOE’s NSDD and General Administration of China Customs (GACC) initiated a series of technical exchange engagements focused on the building of a testing and evaluation capability to strengthen the detection architecture within China’s nuclear security regime. In the context of evaluating a spectroscopic radiation portal monitor that GACC planned to deploy, these exchanges explored best practices in the various components of an effective radiation detection equipment testing and evaluation program. This included all elements required to successfully plan and conduct tests from requirements development through test reporting, as well as test infrastructure and test program management topics. Through this initiative, GACC developed new facets to partnerships with the China State Nuclear Security Technology Center and the China National Institute for Metrology with these organizations offering GACC technical expertise, and testing facilities and resources. Together, this cooperation resulted in comprehensive and effective testing and evaluation capability that has successfully planned and conducted radiation detection and environmental performance tests on a spectroscopic radiation portal monitor for vehicle scanning and a walk-through radiation portal monitor for pedestrian scanning.

Beyond strengthening China’s nuclear detection architecture, this technical exchange approach represents a method to increase the effectiveness of radiation detection equipment, and equipment life-cycle sustainability of other member states. Where resources constrain a state’s ability to maintain a testing and evaluation capability, IAEA Nuclear Security Support Centers and Centers
of Excellence with demonstrated capability in this area could serve as a valuable resource to achieve the same ends: effective detection architectures for all member state nuclear security regimes.

State
United States

Gender
Not Specified

Primary author: HOYT, Joel (Pacific Northwest National Laboratory)
Co-authors: ERCHINGER, Jennifer (Los Alamos National Laboratory); DIETRICH, Richard (Sandia National Laboratories); HAN, Y. (China State Nuclear Security Technology Center); KOLBAS, Pat (Pacific Northwest National Laboratory); LIANG, J. (China National Institute for Metrology); QIAN, L. (General Administration of China Customs); SHERGUR, Jason (Oak Ridge National Laboratory)
Presenter: HOYT, Joel (Pacific Northwest National Laboratory)

Track Classification: MORC: Detection technology development and performance testing
DOWNBLENDING OF HEU GRAPHITE FUEL IN KAZAKHSTAN

The National Nuclear Center of Kazakhstan (NNC) operates an Impulse Graphite Reactor (IGR) with a homogeneous uranium-graphite core. Graphite blocks in the reactor core are impregnated with a water solution of uranyl nitrite with a concentration of ~3.1 grams of uranium per one kilogram of graphite. The enrichment of uranium by the isotope U-235 is 90%. The reactor core consists of immovable and movable parts surrounded by graphite reflectors. The physical start-up of the IGR reactor took place in June 1960, and the energy start-up was in August 1961. In 1967, the IGR reactor was upgraded – the uranium mass in the core was increased from 7.46 kg to 9.0 kg and the diameter of the central experimental channel was enlarged. Since reactor modernization about 2.5 kg of HEU fuel from the first reactor core that was never used in the reactor has been stored at the reactor site. Last year the government of Kazakhstan made the decision to down-blend fresh HEU graphite fuel from the IGR reactor, which is located at the Ulba Metallurgical Plant (UMP) in Ust-Kamenogorsk, Kazakhstan.

The UMP developed a special technology to down-blend the IGR graphite fuel which includes fuel crushing, graphite oxidation, dissolution of uranium oxides, U-235 based correction using depleted or natural uranium, uranium extraction, precipitation, and calcination to oxides. The final product will have an enrichment of about 19.7%. The UMP facility preparations for graphite fuel down-blending should be completed in July or August 2019 and the down-blending process - which may take up to 1 year - will start in October or November 2019. The down-blending will be conducted under the supervision of IAEA safeguards.

The first, irradiated HEU core from the IGR reactor was discharged in 1967 and is currently located in dry storage at the reactor site. The total core weight is about 2,600 kg, and the total mass of uranium (including uranium 235 and 238) is about 7.46 kg. The radionuclide composition is as following: 137Cs, 90Sr, 151Sm, 99Tc, 155Eu, 93Zr, 135 Cs. Since this material was irradiated in a reactor its down-blending at the UMP is not allowed under the current UMP license.

In 2018-2019 NNC conducted a feasibility study for down-blending and final disposition of the irradiated IGR graphite fuel at the NNC site. Based on preliminary results of the feasibility study the dry mixing technology using natural uranium has been proposed as a prospective method for down-blending of the irradiated HEU graphite fuel with the following cementation of the down-blended material for permanent disposition.

This paper will outline the down-blending and disposition plans for both the unirradiated and irradiated HEU located outside the IGR reactor core.
Track Classification:  PP: Minimization, on a voluntary basis, of high enriched uranium within civilian stocks and where technically and economically feasible
An Innovative Approach to Weapons Usable Nuclear Materials Minimization

The U.S. Department of Energy’s National Nuclear Security Administration (DOE/NNSA) Office of Material Management and Minimization (M3) works to minimize civilian stocks of highly enriched uranium (HEU) and separated plutonium globally through the conversion of research reactors from HEU to low-enriched uranium (LEU) fuel and, when possible, removal or disposition of excess weapons-usable nuclear material (WUNM). The majority of uranium-based materials removed by M3 and its predecessor program, the Global Threat Reduction Initiative, have been unirradiated (fresh) uranium or irradiated (spent) uranium based on U-Al or U-ZrH fuel systems. To date, DOE/NNSA has removed or confirmed the disposition of approximately 3,520 kilograms (kg) of fresh HEU and 3,200 kg irradiated HEU.

Although significant progress has been made on HEU minimization, M3 estimates that large quantities of WUNM are still in civil commerce worldwide, much of which is excess to actual needs and is suitable for elimination. However, a large portion of these inventories is difficult to remove or otherwise disposition due to a number of constraints, including:

- Political: sending additional material to various receipt locations—whether in the United States or abroad—can conflict with U.S. or foreign partner priorities or policies;
- Technical: globally, there is limited, or in some cases no, infrastructure capability and/or capacity to eliminate certain types of WUNM; and
- Economic: given current capabilities and capacity, it can be more expensive to disposition certain materials than to pursue long-term storage options which do not result in permanent threat reduction.

To overcome these obstacles, M3 is developing a novel approach to work with foreign partners to eliminate difficult tranches of WUNM in an economic manner where they are located. M3 is developing a mobile platform for stabilizing excess WUNM and converting it into a stable, more proliferation resistant, low-attractiveness waste-form that can be readily disposed in a solid waste disposal facility. The process being developed by M3 builds on U.S. DOE’s advances in the melt-dilute process originally developed for the treatment aluminum spent fuel materials to produce repository-acceptable waste forms. M3 has further adapted this process to cover wide ranging fuel and clad materials and is currently working to stage this process on a mobile platform. The prototype Mobile-Melt Consolidate (MMC) test system being developed leverages the melt processing technology and our understanding of metallurgical phase stability to develop customizable, stable waste forms to meet foreign partners’ solid waste disposal facility performance envelopes. The MMC system aims to provide a new capability to eliminate small quantities of legacy WUNM in-country or in-region rather than commercial transport over long distances. M3 estimates that the MMC capability will be able to address approximately 20-50% of the known excess foreign tranches of WUNM.

This poster will review the issues and challenges associated with the elimination the diverse types of remaining, legacy WUNM and describe in detail the MMC concept and principles. The poster will also highlight the planned capabilities of the prototype MMC test system current being developed by M3 and the associated R&D validation and optimization studies. It will also describe the safety analysis and the regulatory framework for its design and operation. Finally, it will present a notional deployment model framework, highlighting the key points for discussion with foreign partners for its implementation.

State

United States

May 9, 2020
Gender

Not Specified

Primary author:  Mr ROECKER, Scott (DOE/NNSA)
Presenter:  Mr ROECKER, Scott (DOE/NNSA)

Track Classification:  CC: Innovative technologies to reduce nuclear security risks and improve cost effectiveness, where feasible
The Desktop Radiation Portal Monitor – The Ultimate Training Aid for Developing Maintenance Providers

The Desktop Radiation Portal Monitor – The Ultimate Training Aid for Developing Maintenance Providers

Authors: Shane Peper and Craig Stinson (Presenter)

Radiation detection systems and measures are key components of both a State’s nuclear detection architecture and its nuclear security regime. The sustained operation of these radiation detection systems, to detect nuclear and other radioactive material out of regulatory control, requires trained personnel to operate and properly maintain them. Practical considerations and guidance on implementation, as it relates to the sustained operation of radiation detection systems, have recently been published in the IAEA serial publication NSS-30G, “Sustaining a Nuclear Security Regime”, with one of the highlights being the importance of human resource development. The maintenance of a cadre of technicians qualified to maintain radiation detection systems has historically presented challenges to States for various reasons, at both the operational level and the national level (e.g., via a Nuclear Security Support Center). One of the prominent challenges has been access to a functioning detection system for significant time periods to conduct training, and the related limitation on the possible number of trainees at one time. The solution that has been developed to mitigate these training obstacles involves the use of a portable desktop-sized radiation portal monitor, complete with a functional gross counting gamma detector. This solution not only advances the set of technical tools available to train personnel to operate and maintain radiation detection systems, but enables an unprecedented increase in training capacity. This paper will include an overview of this novel maintenance training aid, as well as provide numerous examples of how this tool can be configured to meet the myriad training needs of maintenance staff, including troubleshooting, spare parts testing, etc.

State

United States

Gender

Primary authors: Dr PEPER, Shane (U.S. Department of Energy, Pacific Northwest National Laboratory); STINSON, Craig (Oak Ridge National Laboratory, US Dept of Energy)

Presenter: STINSON, Craig (Oak Ridge National Laboratory, US Dept of Energy)

Track Classification: MORC: Building and maintaining nuclear security detection architecture
Highly Enriched Uranium Radiation Signature Training Device (RSTD)

The U.S. Department of Energy’s National Nuclear Security Administration (DOE/NNSA) Office of Material Management and Minimization (M3) works to minimize civilian stocks of highly enriched uranium (HEU) and separated plutonium from falling into the hands of non-state actors by minimizing and, when possible, eliminating the civilian use of weaponsusable nuclear material (WUNM).

Over the last decade, DOE’s Oak Ridge National Laboratory (ORNL) has developed and fabricated units known as Radiological Signature Training Devices (RSTDs) in various iterations. An RSTD is a device that can emulate the radiation signature of larger masses of Special Nuclear Material (SNM), while using relatively small amounts of the material. This is technically feasible to do because large, solid SNM metal objects shield most of the gamma rays produced.

Specifically, for an HEU RSTD, an equivalent isotropic gamma flux is produced by the use of a small quantity of HEU in a low-density matrix in the shape of icosahedron shell. An RSTD that emulates a 25-kg solid metal sphere composed of 90% 235U consists of 80 HEU triangular source tiles assembled into an icosahedron frame. Each individual titanium source is loaded with HEU material before being welded closed, decontaminated, and leak tested. The 186 keV gamma ray peak from the assembled unit matches that of solid metal sphere of 25-kg of 90% HEU within 10%. The overall unit contains approximately only 240 g of 235U. In addition to the HEU shell, a 1 kg depleted uranium metal source centered in the unit offsets the higher energy gamma emissions. Characterization of the HEU RSTD by gamma spectra measurements at every face and vertex of the assembled icosahedron has shown the unit to be isotropic with very low variability in gamma flux. The modularity of the overall design allows for varied reduced masses of material to be emulated simply by assembling a number of the triangular sources in a different sized frame and/or geometry. The ability to subdivide the sources allows for them to be shipped in five small drums by commercial carrier, making transport substantially easier than movement of a monolithic source.

In the last few years, M3’s Nuclear Material Removal Program has been working cooperatively with ORNL to investigate the technical options for deploying an HEU RSTD to an international partner for its operational use in lieu of using larger quantities of HEU. The technical and operational efficacy of an HEU RSTD has been demonstrated, and M3 and ORNL will continue to find opportunities to leverage the RSTD’s capabilities of emulating HEU, while using very small amounts of SNM. This furthers the shared objectives of furthering HEU minimization policies globally.

State
United States

Gender
Not Specified

Primary author: Ms BRUSIOVSKY, Valerie (DOE/NNSA)
Presenter:  Ms BRUSILOVSKY, Valerie (DOE/NNSA)

Track Classification:  CC: Innovative technologies to reduce nuclear security risks and improve cost effectiveness, where feasible
Establishment of a Master’s Degree Program for Nuclear Security at the Penn State University

To ensure the continued security and safety of nuclear enterprises, the Penn State College of Engineering is formally introducing a nuclear security option in its nuclear engineering master’s program. This unique master’s degree program is designed to educate and train the next generation of nuclear security experts who can actively contribute to improving nuclear and radiological security around the world. This program is the first nuclear security master’s degree program offered in the USA. The Penn State Nuclear Security master’s degree program was created under a grant from the United States Department of Energy and the National Nuclear Security Administration (NNSA). Initial development of the courses was prepared in collaboration with Massachusetts Institute of Technology and Texas A&M University. The Penn State program offers a comprehensive curriculum in nuclear security, primarily for graduate students studying nuclear engineering. This new nuclear security program will be a key resource to help develop the next generation of experts in nuclear security to continue this important work.

The nuclear security program at Penn State is unique and combines the technical, societal, and policy aspects of nuclear security and safety. Students in the program will gain experience with state-of-the-art technologies and be educated/trained in nuclear threat assessment and analysis, global nuclear security policies, and nuclear security system designs. By successfully completing the following five courses, students will receive the designation Master of Science or Master of Engineering with a nuclear security option and significantly expand their expertise on these critical issues.

- NucE 441, Nuclear Security Threat Analysis and Assessment: Nuclear threat assessment and analysis for nonstate actors to nuclear and radiological facilities and supply lines.
- NucE 442, Nuclear Security System Design: Science and engineering associated with the design, evaluation, and implementation of systems to secure nuclear and radiological materials.
- NucE 542, Source and Detector Technologies for Nuclear Security: Theory and technology behind detectors, sensors, and source technologies including portal monitors and field deployable radiation detection systems.
- NucE 544, Global Nuclear Security Policies: Introduce students to global policies and laws for nuclear security that are intended to provide a secure environment for the pursuit of legitimate nuclear activities.

The courses were first offered in 2011, but the new master’s degree option was formally offered to the students starting Fall 2018. Overall details of the Penn State nuclear security master’s degree program will be presented.

State

United States

Gender

Male
Primary author:  Prof. UNLU, Kenan (Penn State University)

Presenter:  Prof. UNLU, Kenan (Penn State University)

Track Classification:  CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomers countries)
The Border Monitoring Working Group
Achievements and History

The Border Monitoring Working Group (BMWG) was established in 2005 by the IAEA, European Union (EU) and United States (US) to promote co-operation between its members and serve as a forum for discussion and exchange of information on plans and programs to be implemented by the members in cooperation with the recipient countries to combat the illicit trafficking of nuclear and other radioactive material that is out of regulatory control. Since its establishment, the BMWG has proven to not only be an effective tool for avoiding duplication and maximizing and targeting resources, but also a forum to address common technical concerns and jointly develop capacity building tools.

For almost fifteen years, the BMWG has proven to be an effective tool for de-conflicting the assistance provided to partner countries thus avoiding duplication and optimizing resources among the group. Among its many accomplishments, the BMWG has coordinated joint training, workshop and exercise activities; developed a progressive and modular front line officer curriculum and a corresponding train-the-trainer concept; coordinated assessment and deployment activities; shared advances in technical issues through providing a collaborative forum for scientific studies and technology applications associated with combating illicit nuclear trafficking; and promoted fixed and mobile detection while extending the impact of increasingly constrained resources. This joint enterprise has developed robust best practices for planning and delivering international assistance for capacity building related to nuclear security.

In its capacity as the coordination mechanism for issues related to illicit trafficking of nuclear and radioactive materials, the BMWG meets twice a year for direct information sharing, coordination and collaboration discussions on respective members’ implementation plans and programs. There are two standing subgroups with a pragmatic focus on training/exercises and technical issues. The subgroups meet on the margins of the biannual meetings and also at other times for special topics and related activities as deemed necessary. Those extra-meetings have focused, for example, on the development of joint training curricula, best practice documents, and detection performance evaluation. The sub-groups report activities and findings to the plenary biannual meetings.

Collaborative efforts resulting in concrete coordinated implementation is a basic tenet of the BMWG actions. The BMWG strives for comprehensive assistance to partner countries through integrated planning and coordinated equipment deployment. In some cases the BMWG jointly engages with a partner country and develops an integrated schedule pulling resources and competences from the different international assistance providers, thereby better accommodating the recipient country’s priorities and needs. Such joint ventures have resulted in, among other things, shared equipment deployments; that is, one partner procures the equipment while another performs the installation or supports maintenance.

Joint projects for curriculum development and training activities have been especially fruitful. Benefits of such joint training include exposure to complementary approaches, global view of international efforts, as well as concrete representation of coordination and integration. The success of this approach is due, in large part, to the contributions from the EC Directorate General Taxation and Customs Union (TAXUD) and other international organizations, such as the World Customs Organization (WCO) and INTERPOL. These curricula for Front Line Officers and Training the Trainers have been successfully delivered locally, regionally, and within the European Nuclear Security Training Centre (EUSECTRA) established at the EC-JRC sites in Karlsruhe, Germany and Ispra, Italy.
Making sure that equipment functionalities and performance are commensurate with end-users needs and constraints is another issue that the BMWG tackles. The group is involved in the testing of the equipment that is used in EU, US and the majority of countries receiving assistance from BMWG members, for the detection of nuclear and other radioactive materials. The BMWG developed a workshop for assisting partner countries build their own capabilities for evaluating detection equipment. The inaugural session of the workshop was hosted by the IAEA at their laboratory in Seibersdorf, Austria in 2018. The BMWG continues to be well positioned to continue to meet the needs of global security by providing practical, beneficial assistance in an agile manner that is responsive to emerging trends and an evolving understanding of capabilities and gaps.

State
Belgium

Gender
Male

Primary author:  Dr ABOUSAHL, Said (European Commission, DG Joint Research Centre)

Co-authors:  Mrs LAUREL, Cotton (US Department of Energy, National Nuclear Security Administration); PELLETIER, Thierry (IAEA); MASSEY, Charles (IAEA); Mrs VON BEHREN, Heather (U.S. Department of State, Bureau of International Security and Nonproliferation); Mr VAN HEESWIJK, Wilhelmus (European Commission, DG Taxation and Customs Union); Mr TOLEUBAYEV, Talgat (INTERPOL, CBRNE Sub-Directorate); Mrs SEMBLAT, Nathalie (Global Affairs Canada, Weapons Threat Reduction Program Division); Mr RICHARDS, Philip (Dept for Business Energy and Industrial Strategy, Global Threat Reduction Programme)

Presenter:  Dr ABOUSAHL, Said (European Commission, DG Joint Research Centre)

Track Classification:  MORC: Building and maintaining nuclear security detection architecture
Gamma Imagers for Nuclear Security and Nuclear Forensics

Natural Resources Canada (NRCan) has responsibility within Canada for mobile survey operations in the event of a nuclear emergency. Our research team, which includes researchers from NRCan, the National Research Council Canada, Defence Research and Development Canada, the Canadian Nuclear Safety Commission, and other Canadian Universities and Federal agencies, has benefitted from close association with the NRCan nuclear emergency response team and has over ten years of experience in conducting mobile radiation survey operations in nuclear security exercises and in support of nuclear security operations.

Radiation detection equipment used in security operations at major events and at borders, and in response to radiation incidents, is typically capable of detection of radioactive substances, with some ability to characterize the strength of the radiation field at the location of the detector, and with some ability to identify the source of radioactivity using the measured energies of emission, but with limited ability to determine the location of the source. In recent years, advances in technology have taken place which have the capability to dramatically improve radiation detection operations. It is now possible to create an image of the field of radiation emitters using the gamma rays which accompany radioactive decay. This radioactivity image can be overlaid on a regular photograph, video, or three-dimensional representation, to dramatically improve response efforts by showing the locations of radioactive sources superposed on locations of objects surrounding the observer.

Gamma imaging technologies have traditionally arisen out of methods developed for medical physics, experimental particle physics and astrophysics applications. This has resulted in the proliferation of different technological approaches, each with different strengths and weaknesses. Some imagers emphasize the ability to identify the radioisotope, or to measure radioisotope ratios, by using materials with superior energy resolution. Other imagers have been developed to have as high sensitivity as possible with low cost materials. Our research group has extensive experience in developing advanced radiation detectors including Compton gamma imagers, specifically for nuclear security operations.

In this presentation we review the current status of gamma imaging worldwide with particular reference to nuclear security and nuclear forensics applications. We discuss quantitative measures which can be used to benchmark different imagers against each other - even if the imagers are based on dramatically different concepts. We present quantitative comparison of the performance of multiple gamma imager designs and technologies, and show which approach is preferable in different scenarios. We present real radioactivity spectra and images, and radioactivity maps, taken in tests and exercises in a variety of conditions: indoor versus outdoor in various weather, mobile versus stationary, single versus multiple viewpoints, point versus multiple or extended sources, discrete observance vs overt observance. We discuss the impact of gamma imaging information products on nuclear security operations and on nuclear forensic investigation. Finally, we give an outlook on future directions for gamma imaging technological and methodological advances.
Primary author: SINCLAIR, Laurel (Natural Resources Canada)

Co-authors: Dr SAULL, Patrick (National Research Council Canada); Dr MCCANN, Andrew (Natural Resources Canada); Dr MACLEOD, Audrey (National Research Council Canada); Mr MURTHA, Nathan (Carleton University); Dr EL-JABY, Ali (Directorate of Security and Safeguards, Canadian Nuclear Safety Commission, Government of Canada); Dr JONKMANS, Guy (Centre for Security Science, Defence Research and Development Canada, Government of Canada)

Presenter: SINCLAIR, Laurel (Natural Resources Canada)

Track Classification: MORC: Detection technology development and performance testing
Radioisotopes such as Cs-137 and Co-60 are used in various medical, industrial, and research applications. This radiological material can be a theft or sabotage target and needs to be protected. This paper will provide an update on the progress of developing an international security standard for devices used in clinical medical settings that contain high-activity radioactive sources. A project team was formed as part of the International Electrotechnical Commission (IEC) to develop the standard. This standard will contribute to reducing the threat of radiological theft and sabotage, and, at the same time, take into full consideration the effect on end-user safety and patient workflow. The contribution of operators, device manufacturers, radioactive source producers, and medical staff in the development of the standard will ensure effective security implementation while minimizing unintended effects of the security measures. The paper will show how an international IEC standard, existing safety standards, and IAEA security guidance can be complementary. While IAEA guidelines primarily focus on the State, competent authorities, and regulatory agencies, the new standard will address device manufacturers and facility operators such as medical clinics, hospitals, universities, and research facilities.

The standard intends to provide practical implementation of sound security measures that can be incorporated into the medical device without affecting the safety and operation of the device, and with minimal impact on device maintenance. This standard also intends to take into account specific medical device and environmental requirements and be flexible enough to provide appropriate levels of protection for a variety device types and configurations.

This paper will address some of the challenges associated with developing such a standard and ways that these challenges may be resolved.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy’s National Nuclear Security Administration under contract DE-NA0003525.
Track Classification: CC: Implementation of national legislative and regulatory frameworks, and international instruments
Experience in Implementing Nuclear Security Culture: Case of Cameroon

The Integrated Nuclear Security Support Plan (INSSP) initial and review missions were carried out in Cameroon in 2012, 2015 and 2018. One of the main nuclear security functional areas was on sustainability which lay emphasis on Nuclear Security Culture. Several recommendations were turned into actions to see to it that the action plan was developed and followed up. National Radiation Protection Agency (NRPA) is championing national Nuclear Security Culture in terms of training workshops and addressed the safety and security of over 500 radioactive sources (sealed sources, unsealed radioactive sources and disused, associated facilities and associated activities) for protecting persons, property and the environment as stated in her mission of Decree number 2002/250. In 2006, Cameroon government expressed her intention to work towards implementing the provisions of the Code of Conduct on the Safety and Security of Radioactive Sources. Its implementation of the code guidance has integrated the safety and security in all regulatory activities. Ratification of the Amendment of the Convention on Physical Protection of Nuclear Material (CPPNM) in 2015 enhanced the integration of safety and security interface, especially the transport of sources. Trainings are conducted on the implementation and operation of the Physical Protection and Security Management with regulators and operators. Regulatory peer reviews and supports implementing inspection regimes in accordance with international safety and security guides are being done at sites with graded approach. Strengthening of Physical Protection at radiation sources facilities have been done. More than 200 national training courses were organized since 2010 with modules of safety and security covered. Modules for Safety and Security are continuously examinied with respect to national needs.

NRPA is part of the national security ad hoc committee for the organization of African Nation Cups since 2016. In order that nuclear security regime remained effective so that it should be sustainable over time at both national and operational levels, NRPA worked together with law enforcement and security officers in a consistent and complementary manner. Training needs assessment was done to clear understanding of the assigned nuclear security functional responsibilities. Identification of those jobs and their related tasks and competencies for which training is required were done. The objective was to come up with nuclear security culture program for promoting, enhancing, and sustaining a strong nuclear security culture. This was done through facilitated practical applications of the nuclear security culture concepts. Some difficulties were encountered at the levels where everyone, or anyone claims or surrenders that that someone would do it. Everyone thought that anyone could do it, but no one understood that everyone would get away from it as radioactive risks are concerned. At the end, everyone accused someone while nobody did what anyone could have done by putting in place a policy or a regulation that could create a national Nuclear Security Committee. NRPA decided to use this as an opportunity, based on the law No2016/015 to coordinate nuclear security culture.

A lot of benefits from implementing the nuclear security culture have been felt. Our Security levels, designed and management systems were enhanced. Improvement of individual performances, shared commitments to nuclear security and employee satisfaction with operators were noticed.

State

Cameroon
Gender

Male

Primary authors: SAMBA, Richard Ndi (National Radiation Protection Agency of Cameroon); SIMO, Augustin (National Radiation Protection Agency)

Presenter: SAMBA, Richard Ndi (National Radiation Protection Agency of Cameroon)

Track Classification: CC: Nuclear security culture in practice with a focus on sustainability
Radiological Material Security in Large Panoramic Irradiators: Lessons Learned

Monday, 10 February 2020 15:15 (15 minutes)

Large Panoramic Irradiators (LPI) are widely used to sterilize medical supplies, food products, spices, cosmetics, and other consumable goods. LPIs typically use a large array of cobalt (Co-60) sources to expose the products to gamma radiation. Co-60 is desirable to terrorist and criminal organizations that are interested in developing a radiological dispersal device (RDD) or radiological exposure device (RED). It is often believed that the LPI Co-60 provides an adequate level of self-protection because of the large radiation dose associated with the source array. This is not true in all scenarios and operational conditions. One typical LPI site with a one-source pool may contain up to 3 million curries (Ci) of cobalt. Approximately 50 commercial irradiators are in operation in the United States and over 200 are in operation worldwide. The United States Department of Energy/National Nuclear Security Administration’s Office of Radiological Security (ORS) is collaborating with LPI facilities to protect Co-60 with the goal of preventing the unwanted removal and misuse of the source material.

This paper will focus on the efforts by ORS to protect LPI sites from a successful theft of Co-60 and will include key lessons learned. These efforts include improving the performance of detection and delay systems to provide local law enforcement the ability to respond to an attack on the facility in a timely manner, which will prevent the removal of the source material. The protection strategy is to develop continuous and balanced layers of security measures. This objective is achieved through security upgrades to access control, intrusion and detection systems, and delay features. ORS is currently working with several LPI industrial partners to implement the protection strategy. ORS worked with LPI partners over several years to develop a mutually acceptable base-line design and implementation process. The design is based on facility assessments, system analysis, component testing, and prudent security practices. For each facility, ORS and partners consider the operational aspects of each facility to develop protection enhancements that minimize any impact to efficiency and effectiveness of the LPI production process.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy’s National Nuclear Security Administration under contract DE-NA0003525.
Session Classification: Physical protection systems: evaluation and assessment

Track Classification: PP: Physical protection systems: evaluation and assessment
Developing Security-by-Design Enhancements for a High-Activity Radioactive Source Stereotactic Radiosurgery Device

Radioisotopes such as Cs-137 and Co-60 are used in various medical, industrial, and research applications. This radiological material can be a theft or sabotage target that requires a certain level of security for adequate protection. The presented work provides an overview of the United States Department of Energy/National Nuclear Security Administration Office of Radiological Security’s In-Device Delay project with Xcision Medical Systems, LLC, on the design of access delay and intrusion detection security enhancements for their GammaPod device. The GammaPod is an innovative stereotactic radiosurgery device used to treat breast cancer. These devices contain high-activity cobalt-60 sources that need to be reloaded periodically, providing challenges when designing robust, sustainable protection elements into a device where those elements may affect the reloading process. This paper will discuss these unique challenges and how the team addressed them.

The paper will also discuss the process and challenges associated with performing a pilot installation of security enhancements at a medical facility and integration of the detection system to the facilities existing alarm system. As part of the installation of security elements, the device must be partially disassembled and is in-operable during the installation phase. In addition, the security stature of the device and sources during the installation process must be addressed. This paper will discuss the coordination effort between various entities including, but not limited to, Xcision Medical Systems, Sandia National Laboratories, the medical facility, and on-site response elements to ensure a successful pilot installation, better protected radiological material, and the continued treatment of patients.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy’s National Nuclear Security Administration under contract DE-NA0003525.

State

United States

Gender

Primary author:  Mr KUCA, Michal (Sandia National Laboratories)
Co-author:  Ms POTTER, Michelle (Sandia National Laboratories)
Presenter:  Mr KUCA, Michal (Sandia National Laboratories)

Track Classification:  PP: Security by design, including in newcomer countries
Sustainability for the Protection of Radioactive Sources

A key challenge to successfully implementing a robust international radiological material security regime is to ensure that the critical knowledge and subsequent training related to the physical security principles of detection, delay, and response can be indigenized and sustained by a State. The Department of Energy/National Nuclear Security Administration Office of Radiological Security (ORS) has developed processes to assist States to develop and implement self-sustaining radiological material security programs. These include knowledge transfer areas of regulations development, principles of physical security, site security plan development, security inspections, transportation security, response, and source search and secure as applied to regulatory agencies, radiological material sites, and law enforcement and response organizations. When these elements are integrated and adopted by a State, it dramatically enhances a State’s ability to appropriately protect radiological materials and to provide continuous long-term risk reduction. This approach has provided partnering States with the capacity and capability to indigenize critical radiological material security measures.

This paper describes how ORS helps build capacity and expertise with partner States to develop sustainable radiological material security regimes. Some examples of successes from partner States will be used to highlight these processes.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy’s National Nuclear Security Administration under contract DE-NA0003525.

State
United States

Gender

Primary author: Mr LOPEZ, Charles (Sandia National Laboratories)
Co-author: Dr EKMAN, Mark (Sandia National Laboratories)
Presenter: Dr EKMAN, Mark (Sandia National Laboratories)

Track Classification: CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
Security requirements to oil well logging radioactive sources: improving security culture

An international concern about radioactive sources after the September 11, 2001 event has led to a strengthening of security. There is evidence that the illicit use of radioactive sources, such as, "radiological terrorism" is a real possibility and may result in harmful radiological consequences for the public and the environment.

Mobile radioactive sources used in industrial applications, such as, industrial gamma radiography, nuclear gauges and oil well logging gauges have become a major concern for regulatory authorities because of the possibility of using them as a "dirty bomb."

Oil well logging is the operation of taking various geophysical measurements in oil wells to evaluate their performance and viability in exploration and production. Gamma sources are used for the density measurement of rock strata around the borehole of an oil well and neutron sources are used for measuring hydrogen levels in rock strata around the borehole of an oil well. Both methods are made by backscatter measurement.

There are in Brazil about 1850 medical, industrial and research installations with radioactive sources. The thirteen oil well logging installations, with radioactive sources classified by IAEA as Safety Category 3 (dangerous to the person) and Security Level C (reduce the likelihood of unauthorized removal of a source), occupy a prominent position due to gamma and neutron radiation emission with high radioactive sources activities, such as, Cs-137 (370 MBq), Am-241-Be (1850 GBq) and Cf-52 (720 MBq).

Safety conditions are well established in these facilities, due to the intense work of Brazilian Regulatory Authority (CNEN). But security conditions, according to the basic concepts of Deterrence (occurs when an adversary, otherwise motivated to perform a malicious act, is dissuaded from undertaking the attempt), Detection (is the discovery of an attempted or actual intrusion which could have the objective of unauthorized removal or sabotage of a radioactive source), Delay (impedes an adversary’s attempt to gain unauthorized access or to remove or sabotage a radioactive source, generally through barriers or other physical means), Response (encompasses the actions undertaken following detection to prevent an adversary from succeeding or to mitigate potentially severe consequences) and Security Management (includes ensuring adequate resources, personnel and funding, for the security of sources) are not yet fully established and incorporated in industrial installations. The main cause observed was the lack of knowledge of workers on security concepts that must be established at the facilities.

Based on IAEA five basic security functions the paper presents some requirements items with practical aspects, such as, using of specific and inviolable barrier (e.g. cage, source housing) to store sources; to confirm the presence of the radioactive sources by periodic checking through physical checks, tamper indicating devices, etc. to be used to improve security culture for oil well logging workers.

State
Brazil

Gender
Male
Primary authors: Mrs GOESSA, EUNÍCIA JOÃO (Agência Nacional de Energia Atómica); Prof. AUGUSTO DA SILVA, FRANCISCO CESAR (Institute of Radiation Protection and Dosimetry)

Presenter: Prof. AUGUSTO DA SILVA, FRANCISCO CESAR (Institute of Radiation Protection and Dosimetry)

Track Classification: CC: Use of IAEA and other international guidelines for building national nuclear security regimes
The considerations and the counter measures of different computer security systems that is used in a research reactor

Computers play a vital role in all aspects during the life time of the research reactor including management, and the safe and secure operation. As the technology advance, the use of computer-based systems at nuclear facilities continues to increase, including the use of many non-standard information technology systems in terms of architecture, configuration, or performance requirements. It is very important that all such systems are properly secured against malicious computer-based actions. At the same time, computer networks and computer-based systems have become a larger target for malicious acts. This includes not only desktop computers, mainframe systems, servers, network devices, but also lower level components such as embedded systems and PLCs (programmable logic controllers).

The requirements of Computer security in nuclear facilities may differ from requirements in other fields. In business applications, only a limited range of requirements is involved; but for nuclear facilities, an entirely different set of considerations need to be taken into account, for example, those affecting e-commerce, banking or even military applications.

According to the IAEA NSS 17, Computer security objectives are commonly defined as protecting the confidentiality, integrity and availability attributes of electronic data or computer systems and processes. By identifying and protecting these attributes in data or systems that can have an adverse impact on the safety and security functions in nuclear facilities, the security objectives can be met.

The security of computer systems [NSS 17] is based on a graded approach, where security measures are applied proportional to the potential consequences of an attack. Categorizing computer systems into zones, and levels is the practical implementation of the graded approach. In any nuclear facility, the plant equipments are classified into two main groups, systems that are important to safety and systems that are not important to safety.

This paper will define the different security levels for the nuclear facility, and list the different considerations for all the computer systems that are used within a research reactor during the reactor lifetime phases according to their security level. For example the reactor protection system (security level 1) needs protective measures that are different from that measures which is needed for office automation systems (security level 5). These protective measures are based on the potential impact on the facility, and to make sure that the different computer systems provide safe, reliable, and deterministic behavior. Also this paper will introduce a survey of existing risks, vulnerabilities, and Consequences of a cyber attack at nuclear facilities.
Primary author: Mr HABASH, Mohamed (Egypt Second Research Reactor - Egyptian Atomic Energy Authority)

Presenter: Mr HABASH, Mohamed (Egypt Second Research Reactor - Egyptian Atomic Energy Authority)

Track Classification: CC: Information and computer security considerations for nuclear security
The Uranium Ore Concentrate Comparative Assessment Database

In 2013, the Government of Canada launched the Canadian National Nuclear Forensics Capability Project (CNNFCP), which undertook various activities aimed at establishing technical and operational frameworks for: (a) a national network of laboratories for undertaking analyses to support nuclear forensics applications; and (b) a national nuclear forensics library (NNFL) cataloguing information and data about radioactive and nuclear (RadNuc) material under Canadian regulatory control.

The task of leading the development of Canada’s NNFL was charged to the Canadian Nuclear Safety Commission (CNSC). Building upon the successes of the CNNFCP, in 2016 the CNSC, in partnership with Atomic Energy of Canada Limited (AECL) (with Canadian Nuclear Laboratories (CNL) as the performing organization), the National Research Council (NRC) and the University of Ottawa, launched the Nuclear Material Signature and Provenance Assessment Capability Development Project (NMS/PAC). The NMS/PAC is a whole-of-government R&D initiative led by the CNSC aimed at developing, enhancing and expanding Canada’s nuclear material characterization and signature data analytics capabilities to support provenance assessment activities for nuclear forensics operations. The scientific and technical outputs of the NMS/PAC feed directly into the Government of Canada’s NNFL, which is maintained and operated by the CNSC.

The nuclear material of focus for the NMS/PAC was uranium ore concentrate (UOC). The objective of the NMS/PAC was twofold: (a) expand the UOC analytical signature reference dataset by producing measurements of a wide range of analytes using various material characterization techniques; and (b) further develop methods to support comparative assessment through the application of data analytics and machine learning techniques. The work of the NMS/PAC has culminated in the establishment of the UOC Comparative Assessment Database (CAD), which is one component of the broader Government of Canada NNFL.

This paper will present an overview of the UOC CAD, including the R&D undertaken as part of the NMS/PAC to support its establishment. Moreover, the paper will outline the rationale behind pursuing an aggressive UOC characterization campaign, as well as the data analytics and machine learning approaches that were developed and incorporated into the UOC CAD to support comparative assessments. The paper will conclude with a discussion regarding the long-term sustainability of the UOC CAD, and how it fits into the broader Government of Canada NNFL concept of operations.

State
Canada

Gender
Male

Primary author: Dr EL-JABY, Ali (Directorate of Security and Safeguards, Canadian Nuclear Safety Commission, Government of Canada)
Co-authors: COCHRANE, Chris (Canadian Nuclear Safety Commission); Dr JOVANOVIĆ, Slobodan (Directorate of Environmental and Radiation Protection and Assessment, Canadian Nuclear Safety Commission); Dr KELL, Tara (Directorate of Environmental and Radiation Protection and Assessment, Canadian Nuclear Safety Commission); Dr DRUMMOND, Christopher (Digital Technologies Research Centre, National Research Council Canada); Dr EL HADDAD, Josette (Energy, Mining and Environment Research Centre, National Research Council Canada); Dr ZHAO, Xiaolei (Department of Physics and A.E. Lalonde AMS Laboratory, University of Ottawa); Dr KIESER, William (Liam) (Department of Physics and A.E. Lalonde AMS Laboratory, University of Ottawa); Dr FRANCISCO, Barbara (Department of Earth and Environmental Sciences and A.E. Lalonde AMS Laboratory, University of Ottawa); Mr MIDDLESTEAD, Paul (Ján Veizer Stable Isotope Laboratory, University of Ottawa); Dr CLARK, Ian (Department of Earth and Environmental Sciences and A.E. Lalonde AMS Laboratory, University of Ottawa); Ms HUYNH, Karen (Atomic Energy of Canada Limited); Dr TOTLAND, Marina (Canadian Nuclear Laboratories); Dr DIMAYUGA, Francisco (Ike) (Canadian Nuclear Laboratories); Dr FOURNEY, Anais (Canadian Nuclear Laboratories)

Presenters: Dr EL-JABY, Ali (Directorate of Security and Safeguards, Canadian Nuclear Safety Commission, Government of Canada); COCHRANE, Chris (Canadian Nuclear Safety Commission)

Track Classification: MORC: Nuclear forensics
Biometrics security and privacy protection

Physical security at nuclear facilities is an important licensing and design consideration. The ultimate objective of the physical protection system (PPS) is to prevent the accomplishment of unauthorized overt or covert actions to nuclear facilities and nuclear materials. When a physical protection system is applied to a nuclear facility or to nuclear materials, its objective is to prevent radiological sabotage of facilities and theft of nuclear materials. Thus an effective system of physical protection also plays an important role in preventing illicit trafficking of nuclear materials.

One of the main pillars of physical protection is controlling personnel access to facilities via Identification technology Systems. Identification technology is changing as fast as the facilities, information, and communication it protects. Recent years have seen a rapid adaptation of using various biometric systems for trusted human automatic recognition and controlling personnel access to nuclear facilities attributed to its high accuracy performance, discriminability, difficulty to be imitated and faked, and stability. Biometrics refers to the physiological or behavioral characteristics of an individual. Many physical characteristics, such as face, fingerprints, iris and behavioral characteristics, such as voice and gait are believed to be unique to an individual. With the exponential growth of using biometric systems, there is an increasing concern that the privacy anonymity of individuals can be compromised by biometric technologies. Unlike passwords and credit cards, which can be revoked and replaced when compromised, biometrics is always associated with a person and cannot be reissued. Biometrics is not secret; the iris of individual can be observed anywhere they look, people leave their fingerprints on everything they touch, and the person will not realize that his/her biometric is disclosed. Biometrics absolutely are sensitive information, therefore biometrics should be protected, because it may be misused by any attacker. To overcome the vulnerabilities of biometric systems, a number of recent strategies can be used such as biometric watermarking, visual cryptography, Steganography and cancelable biometrics. In this article, we provide an overview of various methods for preserving the privacy and security of the individual’s biometrics data.

State

Egypt

Gender

Male

Primary author: Dr ZAHRAN, Osama ( Assoc. Prof. at Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Egypt)

Co-author: Mr ASAKER, Ahmed (Nuclear Security Head for First Egyptian Research Reactor)

Presenter: Mr ASAKER, Ahmed (Nuclear Security Head for First Egyptian Research Reactor)
Session Classification: Innovative technologies to reduce nuclear security risks and improve cost effectiveness, where feasible

Track Classification: CC: Innovative technologies to reduce nuclear security risks and improve cost effectiveness, where feasible
Establishing and Developing an Effective Nuclear Security Culture at Regulatory Bodies

Nuclear security is the system that has responsibilities to prevent, detect and respond to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear or other radioactive substances or their associated facilities. Nuclear security culture is the collection of characteristics, attitudes, and behavior of individuals, organizations, and institutions which serves as a means to support and enhance nuclear security. The paper describes the elements of organizational culture (i.e. beliefs, values, attitudes and behaviors) and the factors that encourage a strong security culture. The paper explains the strategic role that security plays in corporate governance and the need to put organizational management systems in place that support it. In addition, the paper explains what is involved in creating a comprehensive security program that supports security culture. It also emphasizes the need to communicate effectively with staff and develop training programs that help staff understand that security is important and that they have security responsibilities. The paper also emphasizes the need for leadership to create an effective whistleblowing policy, conduct self-assessments of security culture, and effectively manage the relationship with external stakeholders. The paper clarifies the difference between nuclear security culture and nuclear safety culture. Finally, Nuclear security culture is an important component in building a nuclear security system which leads to a robust nuclear security regime. To establish and maintain a nuclear security culture state, organizations and individuals should practice their roles and responsibilities in the right manner. Edgar Schein’s model for working with organizational cultures is of great importance to develop the culture. Assessment and developing of beliefs, attitudes, behavior and management systems lead to more effective nuclear security.

State

Egypt

Gender

Male

Primary authors: ABD EL SAMIA, Mohamed; SHABAN, Sameh (lecturer)

Co-authors: HAZZAA, Mohamed Helmy Mohamed (Egypt); Dr EL-TAYEBANY, Rasha (Egyptian Nuclear and Radiological Regulatory Authority (ENRRA), )

Presenters: ABD EL SAMIA, Mohamed; SHABAN, Sameh (lecturer)

Track Classification: CC: Nuclear security culture in practice with a focus on sustainability
Development of Interactive Tabletop Exercise on National Nuclear Forensics Training Program

Nuclear forensics in Thailand established in 2012 since the Seoul Nuclear Security Summit. The Prime Minister has declared to support the global nuclear security as well as nuclear terrorism mitigation. As a result, Thailand had arranged the ASEAN Regional Forum on Nuclear Forensics on December 2011 and planned to establish a Nuclear Forensics Center. After that, the Office of Atoms for Peace (OAP) has designated to build up nuclear forensics capabilities. There are four main functions to enhancing the performance, which is a response of radiological crime scene, analysis of the signature, development of the database, and strengthens of networks security. The national training program is a key element to support the radiological crime scene management and security networks development in terms of communication among the competent authorities. The training program had conducted in 2017 and 2018. The purposes of the curriculum focus on the law enforcement to gain understanding the role and application of nuclear forensics regarding on nuclear security including establishing the national standard operating procedure (SOP) to respond the unauthorized activities in a timely manner. The program held in three days, composed of lecture method and tabletop exercise. The course syllabus obtained from the lesson learns in various training with IAEA, EU-JRC, and GICNT.

The tabletop exercise was developed by identifying the legal framework, risk assessment, nuclear activities, and incident trafficking database. Four interactive exercises accomplished in several circumstances along with the demonstration of the fictitious scenario and database so that the participants can understand the role and the insight knowledge to establish the SOP. The entitled of the exercises is a metal box, a dead body, a briefcase, and a scrap metal. The metal box intends the networks can understand radiological crime scene management for determination of the origin. The dead body aims to learn a murder investigation related to radioactive material, while the briefcase objects to identify the seized material by interpretation of signatures analysis. In addition, the scrap metal purposes to the inter-agency collaboration to handle with the illicit trafficking involving radioactive material at border control.

After having finished the interactive exercise, we can obtain the SOP. Because of the law enforcement can illustrate the whole process of nuclear forensics in terms of supporting the investigation for nuclear security regarding their responsibilities. In the future, OAP plans to implement the standard operating procedures with the competent authorities not only the law enforcement but also the relevant nuclear security organizations by performing the drill exercise, and field exercise.

State

Thailand

Gender

Female

Primary author: MUNGPAYABAN, Harinate
Co-authors: RUEANNGOEN, AREERAK (Bureau of Technical Support for Safety Regulation, Office of Atoms for Peace, Ministry of Science and Technology, Bangkok, 10900, Thailand); Mrs SRIJITTAWA, Ladapa (Security and Safeguards Technical Support Section Regulatory Technical Support Division Office of Atoms for Peace, Thailand); Ms CHANGKRUENG, Kalaya (Office of Atoms for Peace, Thailand); Mr PHAUKKACHANE, Paphon (Security and Safeguards Technical Support Section Regulatory Technical Support Division Office of Atoms for Peace, Thailand); Ms THONG-IN, Saowaluck (Office of Atoms for Peace)

Presenter: MUNGPAYABAN, Harinate

Track Classification: MORC: Nuclear forensics
Djibouti and the United States Forging a Strong Partnership in Sustaining a Nuclear Security Detection Architecture

Author: Jason Padilla, Osman Hassan Farah

Abstract:
The strong partnership between the United States and Djibouti is a successful representation of a multi-year effort to develop a nuclear detection architecture. Proper implementation and sustainment of a successful nuclear security regime is not a simple endeavor; it requires dedication to building the necessary regulatory framework, and maintenance of the numerous types of required resources. Djibouti’s successful efforts to develop this detection architecture demonstrate that smaller, resource-constrained countries can successfully conduct detection of radiological and nuclear material.

This partnership began as a project to equip Doraleh Container Terminal (DCT) with five radiation portal monitors (RPMs) and ancillary equipment, including handhelds and identification measures. This proved to be only the start of a much larger framework for a nuclear security detection architecture in Djibouti. The United States and Djibouti then partnered to deploy Mobile Detection Systems (MDS). In order to deploy MDS to Djibouti, the equipment needed to be adapted to accommodate Djibouti’s uniquely harsh climate and geological terrain. When the Doraleh Multipurpose Port (DMP) was constructed, Djibouti insisted on developing infrastructure for radiation detection. As a result, there are now five lanes covering all import and export traffic at the DMP. In 2019, two border sites with Somalia and Ethiopia were installed with radiation detection capabilities.

Djibouti now performs a majority of maintenance functions and has developed a strong partnership between Djibouti National Security, Djibouti Customs and Department of Energy. Djibouti has been quick to adopt NSDD’s principles, including starting a Train the Trainer program which will start with an internal assessment of their capabilities. Djibouti has taken the basics of regulatory framework and now through years of cooperation with NSDD, completes the associated administrative processes to ensure the continued success of a nuclear security regime.

This paper will elaborate on the successes, challenges, and lessons learned, in this multi-year cooperation between the U.S. and Djibouti, and also serve as an opportunity for Djibouti to highlight some the structure of their detection architecture.

State
Djibouti

Gender

Primary authors: FARAH, Osman Hassan (Djibouti National Security); PADILLA, Jason (Sandia...
National Laboratories)

**Presenter:** FARAH, Osman Hassan (Djibouti National Security)

**Track Classification:** MORC: Preventing illicit trafficking of nuclear and radioactive material
Sustainability Challenges and Evaluation Recommendations for Handheld Radiation Detection Equipment

Brian Tucker, PhD, PE

Abstract:
Over the past decade, the US Department of Energy’s Office of Nuclear Smuggling Detection and Deterrence (NSDD) has deployed thousands of radiation detection instruments to partner countries for the purpose of detection, location, and identification of radioactive materials at storage facilities, border crossings, seaports, and airports. During this time, challenges have been observed regarding the deployment, operation, sustainability, and repair of these instruments. Specifically, in the areas of sustainability and repair, these challenges have resulted in situations where partner countries lose confidence in the equipment and alter their operations to bypass or discontinue use of the equipment. This presentation will focus on the sustainability challenges encountered, potential solutions, and a method that can be used to evaluate handheld detection instruments prior to making a purchase.

Approximately fifty percent of the maintenance scenarios encountered involve depleted batteries, incorrect settings, or issues that may be easily corrected with a calibration or background measurement. However, with a lack of knowledge or comfort with performing these basic procedures, operators tend to avoid these tasks and, instead, discontinue use of the equipment. To complicate the issue, many sites experience high turnover of operators with minimal succession, no mechanism for the transfer of knowledge, and no budget for continuous training. Additional challenges are introduced due to the international shipping and logistics. Any task ranging from purchasing replacement batteries to a full instrument factory return can become very complex.

Potential solutions to these issues involve participation on the side of both instrument vendors to the partner countries. Instruments should be designed with field serviceability in mind. Vendors should be more forthcoming providing maintenance training, repair manuals, spare parts, and overall better international customer service. Partner countries should develop maintenance management programs where instruments receive adequate preventive and corrective maintenance on a scheduled basis and develop plans that survive staff turnovers. For future purchases of radiation detection instruments, an evaluation method is needed to compare instruments based on a wide variety of factors including operability, performance, sustainability and life cycle costs. New instruments with better technology and design have emerged on the market that advertise better performance and more features. Although not generally publicized, many new instruments are also field serviceable having one or more of the following sustainability features:

- modular, easily-repairable component design
- longer battery life for portable instruments (both operational and lifespan)
- instrument self-diagnostics and state-of-health reports for component failures
- field-upgradable software/firmware

Due to the challenges above, many end users desire field-serviceable instruments, eliminating the need for shipping and logistics back to the vendor. In addition, users need total life cycle cost information to make a more comprehensive comparison between instruments. Unfortunately, sustainability and life cycle cost information is not generally shared prior to procurement and the end user is often burdened with unforeseen maintenance, shipping, and logistics costs to keep the instrument operational. By establishing a method to evaluate instruments for sustainability and estimate life cycle costs prior to procurements, end users can make more informed purchase decisions.

NSDD recognized this gap in information and developed an evaluation method for handheld instruments using an Analysis of Alternatives (AoA) approach. AoA compares several different instrument alternatives based on multiple criteria and provides a final score for each. Although
the focus was on sustainability, the evaluation was expanded into three main “pillars” (operability, performance, and sustainability) and life cycle costs. These pillars are further broken down into more focused categories that may be prioritized and scored, resulting in an overall score for each instrument being evaluated. Analysis scores combined with life cycle costs can be used to make more informed decisions on instrument procurements. An initial evaluation was performed on a set of instruments and will be presented without revealing specific manufacturers and models.

Many proposed solutions to these sustainability challenges require manufacturer cooperation. Specifically, manufacturer assistance is highly valuable when creating and implementing basic and advanced maintenance training. Additionally, manufacturers can recommend shipping and logistics processes to minimize downtime and costs, possibly by using regional distributors or service centers. By enabling partner countries to perform their own maintenance and providing well-defined processes to obtain replacement parts and/or return non-functional instruments for repair, an increase in equipment uptime and longevity may be observed. In addition, enabling member states and partner countries to evaluate instruments will allow them to make future procurements focused on their specific priorities.

State

United States

Gender

Primary author: TUCKER, Brian (Pacific Northwest National Laboratory)

Presenter: TUCKER, Brian (Pacific Northwest National Laboratory)

Track Classification: CC: Innovative technologies to reduce nuclear security risks and improve cost effectiveness, where feasible
Sustaining Nuclear Security Regimes through Continuous Learning Experiences: A Case Study in Knowledge Management Systems Supporting Human Resource Development

Title: Sustaining Nuclear Security Regimes through Continuous Learning Experiences: A Case Study in Knowledge Management Systems Supporting Human Resource Development

Topic Area: Human Resource Development: Knowledge Management

Author(s): Matt Tremonte; Georgia Adams

Abstract:

As Member States plan, implement, and ultimately, sustain their nuclear security regimes, the considerations for developing human resources supporting these regimes are paramount. Human resource development broadly includes programs addressing education, training, and knowledge management. The IAEA’s recently published Implementing Guide, Sustaining a Nuclear Security Regime, highlights the importance of national-level support for assigning resources that help ensure States are able to develop and retain sufficient human resources in the short, medium and long term. Determining what resources are needed to support education, training, and knowledge management is no easy task, and in particular, knowledge management is a practice often overlooked when assigning resources for human resource development. This paper will highlight the importance of implementing continuous learning experiences in knowledge management efforts as part of sustaining a nuclear security regime. Further, this paper will offer approaches for planning and implementing knowledge management systems and measures for States considering and actively developing their own nuclear security knowledge management efforts, and more broadly for their human resource development.

The U.S. Department of Energy / National Nuclear Security Administration / Nuclear Smuggling Detection and Deterrence (NSDD) program has devoted considerable resources to developing and maintaining a knowledge management system that supports partnering countries with their human resource development efforts. This paper will focus on the case study of this Knowledge Management Website (KMW), launched in 2015. The KMW was designed to tie together tools and techniques partner countries could access and use to help support the development of their training, maintenance, and operations programs focused on nuclear security detection. Since the launch, over 200 users from more than 50 countries have signed up and actively use the site.

The KMW is a resource that houses materials such as curriculum for training and procedures for how to maintain and/or operate detection instruments. From the beginning, a focus on products which met “Just In Time” needs was adopted to foster continuous learning experiences relevant to sustaining detection equipment deployed in support of their nuclear security regime. This is an effective strategy in the field of adult learning which evolves away from the “One and Done” mentality attributed to in-person instruction. All IAEA Member States and Nuclear Security Support Centers (NSSCs) are welcome to request access through the KMW page on the IAEA Nuclear Security Information Portal (NUSEC).

This paper will discuss key factors to developing the KMW, including planning considerations for launching the KMW, identifying content which met the model of fostering continuous learning experiences, developing a structured taxonomy for managing this content, communicating to potential users the utility of the KMW, and the importance of incorporating configuration management practices. Additionally, this paper will highlight topics to consider for operating the KMW, including maintaining current documentation, collecting end user feedback, the evolution of the KMW and KMW Mobile App, and the importance of maintaining a close relationship with training.
and curriculum development efforts. Finally, the paper will offer insights into the future of the KMW / KMW Mobile App and provide a summary of lessons learned.

This paper will be structured into sections. The first section will include an introduction and summary of the paper's major points. Section two will include a discussion of the importance of incorporation continuous learning opportunities into knowledge management practices for nuclear security human resource development and introduce the KMW case study. Section three will review the considerations for developing and launching the KMW. The fourth section will review key factors for operating, managing, and evangelizing the KMW, including collecting end user feedback and adapting to training delivery methods and curriculum development needs. Section five will summarize lessons learned from deploying and maintaining the KMW. And finally, section six will provide a conclusion, highlighting future plans for the KMW and knowledge management practices. The topics explored in the paper will be helpful as other States consider approaches to systems and measures for nuclear security knowledge management, and ultimately human resource development.

**State**

United States

**Gender**

Female

**Primary authors:** ADAMS, Georgia (Pacific Northwest National Laboratory); TREMONTE, Matthew (Pacific Northwest National Laboratory)

**Presenter:** ADAMS, Georgia (Pacific Northwest National Laboratory)

**Track Classification:** CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
IAEA NUCLEAR FORENSICS RESIDENTIAL ASSIGNMENTS

R. Kips (Lawrence Livermore National Laboratory / US Department of Energy)
K. Treinen (Lawrence Livermore National Laboratory / US Department of Energy)
E. Kovacs-Szeles (Hungarian Academy of Sciences - Centre for Energy Research – Budapest, Hungary)
K. Mayer (European Commission – Joint Research Centre – Karlsruhe, Germany)
A. Apostol (Horia Hulubei National Institute of Physics and Nuclear Engineering – Bucharest, Romania)
M. Bavio (National Atomic Energy Commission – Argentina)

The IAEA Residential Assignment places a technically qualified nuclear scientist at a leading nuclear forensic laboratory for a period of up to sixty-three working days. The goal of this IAEA program is to enhance the skills and confidence of the resident scientist performing key tasks (such as analytical measurements) in support of a comprehensive nuclear forensic examination. These skills seek to improve the knowledge and expertise available for nuclear forensic examination at the respective home organization. To date, the IAEA Residential Assignment has been hosted by the Hungarian Academy of Sciences Centre for Energy Research (MTA EK), the European Commission’s Joint Research Centre (JRC) and Lawrence Livermore National Laboratory (LLNL) through support of the U.S. Department of Energy’s Office of Nuclear Smuggling Detection and Deterrence (DOE/NSDD). Each host organization applied a somewhat different approach to the implementation of the IAEA Residential Assignment: MTA EK in Hungary centered its Residential Assignment around a team exercise, involving real samples (nuclear fuel pellets) and a fictitious scenarios, and covered all aspects of the investigation, starting from radioactive crime scene management through actual laboratory measurements and the use of a national nuclear forensics library (NNFL). Hungary’s approach to the IAEA Residential Assignment is designed for multiple resident scientists to participate together. Nuclear scientists from Slovakia, Malaysia, Kenya, Czech Republic, Croatia, Bulgaria, Thailand, Kazakhstan and Romania have participated in the program so far. The Joint Research Centre of the European Commission in Karlsruhe, Germany, hosted Andrei Apostol, a non-destructive analysis expert from the Horia Hulubei National Institute of Physics and Nuclear Engineering (IFIN-HH) in Romania, to participate in a scientifically-challenging source characterization project. This research resulted in a scientific publication. For the first Residential Assignment hosted by a U.S. National Laboratory, Marta Bavio, a mass spectrometrist from the National Atomic Energy Commission (CNEA) of Argentina, obtained a deepened understanding of the radiochronometry and trace elemental techniques applied to nuclear forensics samples during her 3-month Residential Assignment with the nuclear forensics group at LLNL. This research stay was framed in the context of an on-going joint sample analysis between DOE/NSDD and CNEA.

The Residential Assignment fosters new or existing nuclear forensics collaborations between the host organization and the home organization of the resident scientists. All resident scientists emphasized that in addition to advancing their analytical skills in the area of nuclear forensics, their experiences in the IAEA Residential Assignments resulted in professional and personal connections that will help them build a long-term international network of nuclear forensics colleagues. Ultimately, the IAEA Nuclear Forensics Residential Assignment is a novel approach to sustainable nuclear forensics capacity building that aims to benefit all parties involved.

State

United States
Gender

Female

Primary author:  TREINEN, Kerri (Lawrence Livermore National Laboratory)

Co-authors:  KIPS, Ruth (Lawrence Livermore National Laboratory);  KOVACS-SZELES, Eva (Hungarian Academy of Sciences, Centre for Energy Research);  MAYER, Klaus (European Commission - Joint Research Centre, Institute for Transuranium Elements);  APOSTOL, Andrei (Horia Hulubei National Institute for R&D in Physics and Nuclear Engineering);  BAVIO, Maria (National Atomic Energy Commission – Argentina)

Presenter:  TREINEN, Kerri (Lawrence Livermore National Laboratory)

Track Classification:  MORC: Nuclear forensics
Performance Testing in the Secure Transport of Nuclear, Radiological, and other High-Risk Materials

Monday, 10 February 2020 15:00 (15 minutes)

A long established methodology for determining the effectiveness of an overall physical protection system (PPS) is through a healthy and robust performance testing program. Performance tests are vital because they provide essential information used in the determination of asset risk and the analysis of protection effectiveness. By establishing and verifying detection, assessment, response, interruption, and neutralization data, one can determine baseline protection effectiveness and consider upgrade scenarios and improving effectiveness. Performance testing also addresses the needs of multiple stakeholders, including the vulnerability assessment teams, site/facility personnel, and safety, and provides management with an independent, objective assessment of overall physical protection systems.

Performance testing can be applied to any layer of PPS at a fixed site or any mode of transport. In an example of road transport by box truck, we can test one layer of a PPS. In this example, we will focus on the delay associated with breaching times of different types of tie down mechanism used to secure containers while in transit. This test will be limited scope in nature and will use three different methods of breaching (mechanical, ballistic, and explosive). During the test, we will attempt to breach the tie down chains and the locking mechanism multiple times with each method.

At the conclusion of the test, objectives and evaluation criteria will be analyzed to ensure the system is performing as required, deficiencies are identified, and stakeholders are provided with feedback/results. For example, the results from this particular set of tests can be used to determine figures of merit associated with delay mechanisms to determine response time needs in relation to the delay associated with breaching the tie downs.

This paper and presentation will discuss adapting fixed facility performance testing plans to transport, best practices for transport performance testing, and how to implement analyses in to protection strategies.

State

United States

Gender

Primary authors:  Mr VERNER, Greg (Y12 National Security Complex); Mr STOCKWELL, G. Scott (Y12 National Security Complex); Dr MILOJEVICH, Allyn (Y12 National Security Complex)

Presenters:  Mr VERNER, Greg (Y12 National Security Complex); Dr MILOJEVICH, Allyn (Y12 National Security Complex)

Session Classification:  Physical protection systems: evaluation and assessment
Track Classification: PP: Physical protection systems: evaluation and assessment
Joint Sample Analysis on Selected Uranium Ore Concentrates and Nuclear Forensics Library Exercise

R. Kips (Lawrence Livermore National Laboratory / US Department of Energy)
R. Lindvall (Lawrence Livermore National Laboratory / US Department of Energy)
N. Marks (Lawrence Livermore National Laboratory / US Department of Energy)
V. Gluchshenko (Institute of Nuclear Physics – Kazakhstan)
A. Okubo (Japan Atomic Energy Agency – Japan)
E. Kovacs-Szeles (Hungarian Academy of Sciences Centre for Energy Research)

The IAEA’s recent publication on Development of a National Nuclear Forensics Library: A System for the Identification of Nuclear or Other Radioactive Material out of Regulatory Control, reemphasizes the rationale for the development of a national nuclear forensics library (NNFL) and addresses how a country may use such a national system in investigations of nuclear and other radioactive material out of regulatory control. According to this publication, it is important for a country to determine whether a nuclear forensics sample is consistent with its domestic nuclear material holdings. As a system for the identification of nuclear or other radioactive material, a national nuclear forensics library, can facilitate interpretation of findings and assist in this determination.

Lawrence Livermore National Laboratory (LLNL), through the U.S. Department of Energy’s Office of Nuclear Smuggling Detection and Deterrence (NSDD), has partnered with the Republic of Kazakhstan’s Institute of Nuclear Physics (INP), the Japan Atomic Energy Agency and the Hungarian Academy of Sciences Centre for Energy Research (MTA-EK) on a joint sample analysis involving a set of uranium ore concentrate (UOC) samples. The sample set contained five UOC powder samples of known origin and a sixth sample of unknown origin (blind sample). The objective of the joint sample analysis exercise was to characterize the uranium ore concentrate samples according to a well-developed analytical plan, and use the measured material characteristics to populate a nuclear forensics library. This library is then used to establish potential links between the blind sample and the samples of known origin. The four participating laboratories compared data and analysis methods, and shared best practices on the implementation of a national nuclear forensics library.

As the largest single producer of uranium in the world, Kazakhstan has a targeted interest in understanding the measurable characteristics associated with the uranium ore concentrate (UOC) it produces. The planned Kazakhstan NNFL will include data resources and expertise on the wide range of nuclear and radioactive materials present in Kazakhstan. UOC is signature-rich and is therefore a good material to target for inclusion in an NNFL. The first data resource for the Kazakhstan NNFL will therefore be UOC.

State

United States

Gender

Female
Primary author:    KIPS, Ruth (Lawrence Livermore National Laboratory)

Co-authors:       LINDVALL, Rachel (Lawrence Livermore National Laboratory); Dr MARKS, Naomi (Lawrence Livermore National Laboratory, U.S. Department of Energy); GLUCHSHENKO, Viktor (Institute of Nuclear Physics – Kazakhstan); OKUBO, Ayako (Japan Atomic Energy Agency); KOVACS-SZERES, Eva (Hungarian Academy of Sciences, Centre for Energy Research)

Presenter:        KIPS, Ruth (Lawrence Livermore National Laboratory)

Track Classification:    MORC: Nuclear forensics
Insider Analysis in the Secure Transport of Nuclear, Radiological, and other High-Risk Materials

The Insider Quantification and Ranking Process (IQRP) is an assessment tool that effectively and accurately identifies and documents the potential negative effects an insider can have on the site’s protective posture. This analysis involves conducting interviews, physical protection analyses, validating or invalidating current analysis documentation or assumptions. The “risk-based” interview questionnaire aids in the quantification, or scoring, of insiders based off access, authority, and knowledge. The scoring tool allows analysts to transition from qualitative information to quantitative data, similar to the Kepner-Tregoe process, to further prioritize the analysis results based on the criteria of significance. The interview questionnaire is designed to validate, or invalidate, assumptions associated with job categories and associated capabilities. Capabilities include access, authority, and knowledge. Questions for access and authority tend to be closed-ended (black and white), while knowledge is more open-ended (gray). After the questionnaire is complete, answers are scored based on a ranking matrix. To be clear, this tool is designed to assess currently employed personnel by position, their potential to become an inside threat, and how dangerous an insider threat they could post. It does not identify individuals that are nefarious insiders. After completing the assessment, facility manager could better determine the critical positions and consider ways to implement mitigation strategies, such as a Human Reliability Program (HRP). Until now, this process has mostly been tested and implemented at static sites for site specific physical security. This paper will discuss its application to secure transport, including adaption and potential adoption by secure transport operators.

The major benefit of an engagement focusing on an assessment tool rather than implementation of personnel security or an HRP is that it requires minimal costs aside from staff time and no capital investments. Background screenings, periodic monitoring, and continuing medical examinations through an HRP require major advancements. The IQRP simply requires the time of several staff members. It is an enlightening evaluation in that management often does not see the way that insider potential varies from individual to individual and from position to position. This assessment tool provides quantitative data that facility management can use when considering how to address the concerns over insider threat. These benefits make it especially beneficial in the international community, which may not have the resources to invest in large-scale HRP or other insider mitigation programs.

This paper will describe the process and highlight how it can be applied to secure transport, especially when considering the role of contractors, coordination between the transporter and local law enforcement, and the role of response.

State
United States

Gender
Female

Primary authors: MILOJEVICH, Allyn (Y12 National Security Complex); Ms PARRILLA, C. Meghann (Y12 National Security Complex); Ms SUMNER, Machelle (Y12 National Security Complex)
Presenters: MILOJEVICH, Allyn (Y12 National Security Complex); Ms PARRILLA, C. Meghann (Y12 National Security Complex)

Track Classification: PP: Insider threats
EVALUATING RADIOCHRONOMETRY BY SINGLE COLLECTOR MASS SPECTROMETRY FOR NUCLEAR FORENSICS: A MULTI-INSTRUMENT STUDY

EVALUATING RADIOCHRONOMETRY BY SINGLE COLLECTOR MASS SPECTROMETRY FOR NUCLEAR FORENSICS: A MULTI-INSTRUMENT STUDY

K. Samperton (Lawrence Livermore National Laboratory / US Department of Energy)
K. Treinen (Lawrence Livermore National Laboratory / US Department of Energy)
R. Lindvall (Lawrence Livermore National Laboratory / US Department of Energy)
J. Wimpenny (Lawrence Livermore National Laboratory / US Department of Energy)
M. Bavio (National Atomic Energy Commission – Argentina)
A. Gaffney (Lawrence Livermore National Laboratory / US Department of Energy)
R. Williams (Lawrence Livermore National Laboratory / US Department of Energy)

Radiochronometric age constraints are a foremost signature in assessing the provenance and processing history of nuclear material out of regulatory control. When possible, the application of multiple radiochronometers can provide increased confidence for interpreting age-dating results in a nuclear forensic examination. Radiochronometric data has traditionally been acquired via multicollector mass spectrometry, a relatively expensive and sophisticated analytical technique. We therefore explored the potential of performing age-dating by single collector mass spectrometry. If achievable, single collector radiochronometry would be a valuable contribution given these instruments’ widespread availability compared to multicollector mass spectrometers, thereby expanding radiochronometry to a broader range of the international forensic community. Such a development would ideally result in the increased acquisition of accurate and reliable age information that will further bolster the global response to nuclear interdictions.

Our approach to evaluating the feasibility of this technique for radiochronometry consisted of a multi-instrument intercomparison experiment, in which single and multicollector mass spectrometers were used to characterize uranium certified radiochronometry standards in parallel. The exact same radiochronometry samples, isotopic tracers, quality control reference materials, and data reduction algorithms were used in both the production and processing of data generated by each instrument, allowing for direct comparison of isotopic and age-dating results amongst the various mass spectrometer designs. Our findings clearly demonstrate that single collector mass spectrometry can be successfully implemented to obtain high quality radiochronometric data. Certified radiochronometry standard ages and isotopic data from single collector instruments are consistent with those from multicollector instruments. While multicollector mass spectrometers ultimately generate the most precise radiochronometric and isotopic data, single collectors can be used to accurately constrain the age of nuclear material.

State
United States

Gender
Female

May 9, 2020
Page 660
Primary authors: SAMPERTON, Kyle (Lawrence Livermore National Laboratory); TREINEN, Kerri (Lawrence Livermore National Laboratory)

Co-authors: LINDVALL, Rachel (Lawrence Livermore National Laboratory); WIMPENNY, J. (Lawrence Livermore National Laboratory); BAVIO, Maria (National Atomic Energy Commission – Argentina); GAFFNEY, Amy (Lawrence Livermore National Laboratory); WILLIAMS, Ross (Lawrence Livermore National Laboratory)

Presenter: TREINEN, Kerri (Lawrence Livermore National Laboratory)

Track Classification: MORC: Nuclear forensics
Meeting the Needs of NSSCs: A Modular Approach to Train-the-Trainer

Meeting the Needs of NSSCs: A Modular Approach to Train-the-Trainer
Authors: Shane Peper (Presenter) and Joan Wilson

The development of human resources [and the maintenance of those resources] to support a State’s nuclear security regime has been identified as a national level sustainability objective (i.e., Objective #6) in the recent IAEA publication NSS-30G, “Sustaining a Nuclear Security Regime”. In addition, this document denotes an operational sustainability objective for developing and maintaining nuclear security competences (i.e., Objective #4), which is typically done through education and training programs. In order to meet the demand for developing and maintaining an adequate number of personnel that possess the requisite nuclear security competences, many States have established Nuclear Security Support Centers. Based on the needs of a State’s nuclear security regime, NSSCs can be tailored to provide support in areas such as scientific support, technical support, and/or human resource development (HRD).

HRD programs often incorporate train-the-trainer (T3) programs to qualify instructors to train in various nuclear security disciplines (e.g., detection, response, physical protection). Typically, these T3 programs are each aligned with a specific nuclear security course/topic, and more often than not, focus on developing basic instructor skills rather than focusing on providing instruction on how to train a specific nuclear security course/topic. This paper will outline a new approach to T3 program development that uses a systematic approach to training (SAT) to develop interactive modules focused on developing the specific skills needed to effectively train foundational courses in various nuclear security disciplines, as well as providing instruction encompassing basic instructor skills. In addition to describing the general approach to the design of the T3 program, additional anecdotal evidence will be presented on how this approach has already been successfully used to support instructor development at select NSSCs and international nuclear security training centers.

State
United States

Gender

Primary authors: Dr. PEPER, Shane (U.S. Department of Energy, Pacific Northwest National Laboratory); WILSON, Joan (Pacific Northwest National Laboratory)

Presenter: Dr. PEPER, Shane (U.S. Department of Energy, Pacific Northwest National Laboratory)

Track Classification: CC: Capacity building (e.g. human resource development and sustain-
ability, nuclear security education and job-specific performance training including for newcomer countries)
Quantitative Model for Assessing Facility Level Radiological Risk

Abstract

The safety and security of a radiological facility share a common objective—ensure the protection of population and environment from undue radiation hazard. Historically, many analytical methods have been developed and implemented to support safety-based risk assessment and decision analysis. Adapting and extending risk assessment to security applications has been limited because of the adaptive nature of the sub-state actors and the lack of historical data of terrorist attacks on radiological facilities. Given the definition of an adversary or terrorist (i.e., any individual performing or attempting to perform a malicious act) the proposed tool utilizes a combination of probabilistic methods and pathway analysis to define terrorist, or more broadly, adversarial attack scenarios. The motivations behind an asset choice for stealing or sabotage, will influence the type of pathway the adversary is most likely to choose to achieve their goals. Bearing in mind that everything is vulnerable to some degree, even when the controls are in place and performing as intended; the threat scenarios were mapped across a spectrum of vulnerabilities including natural disasters, crime in the area and power disruption in the region of interest. Nuclear security culture assessed through surveys yielded a numerical value to reflect the importance of the human dimension in risk assessment. It is one factor that reflected the synergy between threat and vulnerability, lending the greatest weight towards the calculation of the risk metric, specific to the radiological facility. For risk analysis to be meaningful, it should include both the frequency and magnitude components. In the advent of a successful radiological theft and a hypothetical detonation and dispersion of radioactive material; the probable magnitude loss, unique to the threat included Loss of Life (LL) and Economic Loss (EL) as two separate variables expounding the severity of damage. The triplet definition of risk, structured as a set of threat, vulnerability and consequences was used to construct a single composite number by weighing the threat scenario probabilities, relative attractiveness and characteristics of the radioactive material, multiple parameters elevating vulnerability of source security and the consequence net loss. The proposed methodology and the risk program model made a suitable platform to compare the baseline risk index of the radiological security of different facilities in the United States. Risk metric, when converted into a qualitative scale delivered a better clarification and linkage between understanding risk and making decisions towards radiological security improvements. The contribution of the proposed research is significant because it is the next step towards development of a new tool in the field of radiological source security—one that is expected to introduce, analyze and numerically test a methodology that yields a facility level risk index.
**Primary authors:**  RANE, Shraddha (Purdue University);  HARRIS, Jason (Purdue University)

**Presenter:**  RANE, Shraddha (Purdue University)

**Track Classification:**  PP: Risk-informed approach to the security of radioactive material in use and in storage
Vulnerability Assessment to Several Nuclear Facilities: an Effort to Improving Nuclear Security Capability in Indonesia through Higher Education

Indonesia has a long experience with nuclear technology, since a first Indonesian national committee began to investigate nuclear fall out in 1954. But, nuclear security is a relatively new issue in Indonesia, and hence several nuclear facilities in Indonesia, including hospitals and industries utilizing radiological material, is operating in a low security. To face up the security problem, Nuclear Engineering Program of Universitas Gadjah Mada has been analyzed security vulnerability of several facilities. There are several studies related to the nuclear security of nuclear medical unit in hospitals in order to improve their physical protection systems. The study is not only limited to the present facilities but also to the estimated facilities which will be built in the future. Recently, several studies on advanced nuclear reactor’s security systems have been also conducted to anticipate when the first advanced nuclear reactor is chosen to be utilized in Indonesia.

State

Indonesia

Gender

Male

Primary author: Mr FERDIANSJAH, Ferdiansjah (Universitas Gadjah Mada)

Co-authors: PUTERO, Susetyo Hario (Universitas Gadjah Mada); Mr SANTOSA, Haryono Budi (Universitas Gadjah Mada)

Presenter: Mr FERDIANSJAH, Ferdiansjah (Universitas Gadjah Mada)

Track Classification: PP: Physical protection systems: evaluation and assessment

This paper summarizes preliminary results of a joint US-Japan study to establish, through science-based study, a mutual understanding of the risk from non-state actors conducting malicious acts involving nuclear material and facilities. The ultimate goal of this study is to develop a methodology to evaluate, assess, and reduce the risk associated with hypothetical (i.e., not specific existing) nuclear facilities, fuel cycles, and waste products related to nuclear materials, and to formulate nuclear security systems as appropriate.

To date, the focus of this study has been on quantifying the intrinsic risk associated with the theft and sabotage of nuclear materials at facilities that handle these materials. Concept to reduce risks will be evaluated later in the study. Intrinsic, or internal, risk reduction factors include gross weight, radiation dose rate, processing complexity including chemical dilution, heat content, and other material properties that either provide self-protection or increase the required mass of material that must be stolen to produce an effective malicious act. The sum of these factors may be expressed as the overall material attractiveness of the nuclear material. Extrinsic, or external, risk factors include physical measures, such as containers, structures, buildings, guards, and other external mitigating barriers. Extrinsic factors also include administrative controls, such as procedures, regulations, training, etc. that define and defend the use of physical controls.

Theft and sabotage define the two broadest categories of malicious acts. These two categories are divided into nuclear and radiological malicious acts, and the four resultant categories are subdivided into ten specific radiological or nuclear malicious acts. The malicious acts considered range from radioactive dispersal due to acts of sabotage, to a radiological dispersal device, to a nuclear explosive device.

Three levels of adversary are considered, each with varying capability to commit various malicious acts identified in the study. In this initial phase of work, nineteen nuclear materials and seven nuclear facilities are evaluated. These are nuclear materials and nuclear facilities that are common to the commercial nuclear industry in the US and Japan.

For each potential malicious act, metrics were identified. Metrics are only considered if they can potentially provide an effective barrier to one of three adversary types in using a nuclear material or nuclear facility in a malicious act. In the case of theft of nuclear material, the metrics selected are gross weight, radiation dose rate, processing complexity, bare critical mass, and heat content. Each nuclear material is graded against these five metrics. This provides the overall attractiveness of the nuclear material to an adversary, which is a measure of the probability that the adversary could successfully execute the malicious act in question. The study also considers the overall consequences of such malicious acts, including number of deaths, number of injuries, and the economic impacts of each act.

The Goal 9 study is being conducted at the request of the United States Department of Energy/National Nuclear Security Administration (DOE/NNSA) and at the request of the Japanese Ministry of Education, Culture, Sports, Science, and Technology (MEXT).
Gender

Male

Primary author:  HORI, Masato (JAEA)
Co-author:  Dr BATHKE, Charles (Los Alamos National Laboratory)
Presenter:  HORI, Masato (JAEA)

Track Classification:  CC: Advances in nuclear security research and development; international cooperation on nuclear security research
NGO-Government Partnership in Strengthening Radiological Security

Nongovernmental organizations (NGO) have played and continue to play a very important role in supporting governments’ efforts aimed at strengthening nuclear security at national, regional, and international level by: 1) promoting dialogue between various stakeholders; 2) building national capacities through education and training, and 3) creating partnerships with government bodies which license and regulate civilian use of radioactive materials.

The authors, who represent both a nongovernmental organization and national regulating bodies, believe that through such partnerships NGOs can complement governments’ efforts to strengthen controls on radioactive sources and observe the IAEA Code of Conduct on the Safety and Security of Radioactive Sources. The authors will support this view by analyzing two types of partnerships between the James Martin Center for Nonproliferation Studies (CNS) and the governments of Moldova, Georgia, and between CNS and Malaysia.

The first case involves CNS cooperation with several post-Soviet countries in tracking down orphan and Soviet legacy radioactive sources using innovative methods and techniques. These include network and social media analysis and online survey tools, in combination with other established methods, such as physical and administrative searches. Such collaboration, particularly in Moldova, has produced tangible results and helped its government gain control of several hundred orphan radioactive sources.

The second case involves a partnership between CNS and the government of Malaysia to improve the transportation security of industrial radiography sources. CNS is working with its Malaysian partner to improve transportation security with the help of technical tools (such as geospatial analysis) and enhancements to security culture.

The paper will analyze these partnerships using the following criteria: 1) time efficiency; 2) project costs; 3) ability to meet project goals (quantitative and qualitative measurements); 4) end-user satisfaction; 5) project team satisfaction; 6) project sustainability.

The paper will address the successes and challenges of such partnerships and how they vary depending on the stakeholders and countries involved. The paper will conclude with recommendations on how to expand and strengthen NGO-government partnerships in the field of radiological security and how creating more such partnerships would benefit nuclear and radiological security.

State

United States

Gender

Female

Primary author: KALININA-POHL, Margarita (Center for Nonproliferation Studies, Middlebury Institute of International Studies)

Co-authors: KADER IBRAHIM, Sabariah (Malaysia Nuclear Agency); POMPER, Miles (James Mar-
tin Center for Nonproliferation Studies); BALAN, Ionel (National Regulatory Body); Mr DUITSMAN, Michael (James Martin Center for Nonproliferation Studies)

**Presenter:** KALININA-POHL, Margarita (Center for Nonproliferation Studies, Middlebury Institute of International Studies)

**Track Classification:** CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
Abstract

A master degree program in Engineering Physics with specialization in Nuclear Security at the Department of Nuclear Engineering and Engineering Physics, Faculty of Engineering Universitas Gadjah Mada has been established in 2016. Several effort have been done for sustaining the program. Analysis of strength-weakness-opportunity-threat (SWOT) has been developed to formulate a new strategy for sustaining effort. Five component of academic capacities have been used for identification criteria. Two strategies could be taken as priorities, such as (1) Collaboration with regional partner to promote the program (increase student body) and (2) Promoting collaboration with the member of IConSEP for human resource development.

Introduction

Elements of a education process can be classified in four components, input, process, output, and outcomes. Students enrollment have been conducted each year. A selection system is strictly used to ensure getting qualified students. Higher education has two activities, learning and research activities. Outputs from the education are alumni, research products and other intellectual property rights. Outcomes from the education are acceptability and recognition from the public and society.

A good education system should fulfill the need of graduates from the society. Jobs market analysis and feed back advisory from stakeholders are needed for sustaining the education system. Nuclear security education has a important role in providing professional human resources for
regulatory body and other organizations with nuclear security responsibilities. Allocating sufficient human resources is part of contribution for the sustaining the nuclear security regime. A strategic approach for sustaining the nuclear security education at Universitas Gadjah Mada has been developed based on the analysis of existing academic capacities and performance: curriculum, faculties and facilities, quality assurance and collaboration. External feedback evaluation and advisory are necessary in the academic planning in order to obtain conformity between student outcomes and user needs.

**Curriculum**

Curriculum is a basis framework of learning process so that students can acquire professional competencies. A curriculum should be developed based on sharpening specifications as a result of the optimization between vision of science and the needs of the job market. Master degree program at the Department of Nuclear Engineering and Engineering Physics, Faculty of Engineering, Universitas Gadjah Mada has been established in 2016. Curriculum program consist of 20 credits for fundamental courses (general education, mathematics, fundamental science and engineering), 8 credits for thesis and 12-22 credits for specialization courses. Four specialization program have been offering: Instrumentation system, Renewable Energy System (RES), Nuclear Technology System (NTS) and Nuclear Security System (NSS). A new specialization in Nuclear Safety and Security System (NS&SS) has also been developed in 2019. It is an integration between the specialization in Nuclear Technology System and Nuclear Security System.

Table 1. Specialization in NTS, NSS and NS&SS

<table>
<thead>
<tr>
<th>Category</th>
<th>Nuclear Technology System</th>
<th>Nuclear Security System Engineering</th>
<th>Nuclear Safety-Security System Engineering</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Course Title</td>
<td>Course Title</td>
<td>Course Title</td>
</tr>
<tr>
<td><strong>DE</strong></td>
<td>Nuclear Reactor System Engineering</td>
<td>Nuclear Security System Design (**)</td>
<td>Nuclear Security System Design (*)</td>
</tr>
<tr>
<td>12 Credits</td>
<td>Nuclear Safety, Security &amp; Safeguard System Engineering (**)</td>
<td>Nuclear Material Accountability and Control</td>
<td>Nuclear Safety, Security &amp; Safeguard System Engineering (*)</td>
</tr>
<tr>
<td></td>
<td><strong>Total:</strong> 3</td>
<td><strong>Total:</strong> 3</td>
<td><strong>Total:</strong> 3</td>
</tr>
<tr>
<td><strong>FE</strong></td>
<td>Nuclear Material Processing System Engineering (**)</td>
<td>Nuclear Security Instrumentation</td>
<td>Nuclear Fuel Cycle and Radioactive Waste Management (**)</td>
</tr>
<tr>
<td>3 - 9</td>
<td>Radiation Protection Engineering</td>
<td>Nuclear Security Legal Framework</td>
<td>Nuclear Safety Analysis Method</td>
</tr>
<tr>
<td></td>
<td>Radiochemistry</td>
<td>Nuclear Forensics (**)</td>
<td>Nuclear Forensics (**)</td>
</tr>
<tr>
<td></td>
<td><strong>Total:</strong> 3</td>
<td><strong>Total:</strong> 3</td>
<td><strong>Total:</strong> 3</td>
</tr>
<tr>
<td><strong>FE</strong></td>
<td>Human Factors and Nuclear Safety-Security Culture (**)</td>
<td>Human Factors and Nuclear Security Culture (**)</td>
<td>Computer and Information Security</td>
</tr>
<tr>
<td>3 - 12</td>
<td><strong>Total:</strong> 3</td>
<td><strong>Total:</strong> 3</td>
<td><strong>Total:</strong> 3</td>
</tr>
</tbody>
</table>

NC: Number of credits; DE: Directed Elective (Specialization) Courses; FE: Free Elective Courses

Figure 2: enter image description here

Strengthening the existing curriculum with nuclear security subjects has been developed through specialization courses (Table 1). Curriculum has been already optimized based on the adequateness of resources. There are several similarities between specialization courses for Nuclear Technology System (marked with (J on Table 1), and between specialization courses for Nuclear Security System Engineering and Nuclear Safety-Security System Engineering (marked with ( on Table 1).
Faculties

Adequate faculty development with the nuclear security subjects has been conducted through several activities, such as participation on INSEN meeting, PDC on Nuclear Security, Nuclear Security Educator Study Tour, and workshop on Nuclear Security Education.

Two workshops on nuclear security for the faculty member have been conducted in 2014 and 2015 with the support from Partnership for Nuclear Security. Both workshops have been conducted for improving educator’s knowledge and understanding on nuclear security. Evaluation has been done to capture the understanding of participants at the beginning phase and after their participation on the workshop. Several questions have been formulated related with the subjects of workshop (Figure 3 and Figure 4).

Figure 3. Grade of understanding before and after participation in the workshop 2014
Before their participation on the workshop in 2014, the participants explained that their understanding on several subjects has graded close to “good” (Figure 3), i.e. subjects no 1 (“Understanding broad picture of NS”), subject no 2 (“NS threat by non-state actors”), and subject no 6 (“Definition of NS”).

![Graph showing grade of understanding before and after participation in the workshop 2015](enter image description here)

**Figure 5: enter image description here**

Figure 4. Grade of understanding before and after participation in the workshop 2015

After completion of two workshop 2104 and 2015, the understanding on nuclear security of the faculty member have been increased significantly.

**Facilities**

Department of Nuclear Engineering and Engineering Physics has one laboratory which can be used to support the nuclear security education (laboratory for nuclear energy technology). Providing adequate equipment for laboratory exercise and research have been developed in 2015 through equipment grant from Chevron Indonesia and 2018 through equipment grant from the IAEA (Figure 5).
The existing radiation detection equipment are adequate to conduct laboratory exercise and research on nuclear security subjects.

**Quality Assurance**

Assessment system for academic quality consist of two track, internal quality assurance system and external assurance system. The internal quality assurance system has been developed by the university. Internal quality audit has been conducted each year (on August). External quality assessment will be conducted through national accreditation every five year.

**Collaboration**

Several cooperation with international partner have been signed, such as Texas A&M Engineering Experiment Station Nuclear Security Science and Policy Institute (NSSPI) USA, Institute Telekom des Mines de Nantes, The Board of Regents of The University Systems of Georgia by and on behalf of the University of Georgia Center for International Trade & Security USA, and King’s College London. Several activities have also already hold, such as nuclear security workshop, staff mobility, joint curriculum development, guest lectures, and faculty development courses. Collaboration with local partner (national) is currently only with the National Regulatory Body (BAPETEN) with several activities on nuclear security workshop and training. Other potential partner for collaboration are several institution which are member of the Indonesia Center of Excellent for Nuclear Security and Emergency Response (IConSEP).

**Strategy Development**

Analysis of strength-weakness-opportunity-threat (SWOT) have been developed to identify new strategies for sustaining the program. Identification of each aspect (strength, weakness, opportunity and threat) has been summarized in Table 2.

Table 2. SWOT Analysis
Several strategies (SO, ST, WO, and WT) have been developed based on the identification of SWOT components (Table 2). Two strategies could be taken as priorities, such as (1) Collaboration with regional partner to promote the program (increase student body) and (2) Promoting collaboration with the member of IConSEP for human resource development.

Summary

The strategic approach for sustaining the master degree program in nuclear security at Universitas Gadjah Mada has been developed based on SWOT analysis using in five criteria, curriculum, faculties, facilities, quality assurance system and collaboration. Two strategies could be taken as priorities, such as (1) Collaboration with regional partner to promote the programme (increase student body) and (2) Promoting collaboration with the member of IConSEP for human resource development.

Acknowledgment

Gratefully thank and acknowledgements are expressed to the agency by giving support to the authors to participate on this conference (International Conference on Nuclear Security 2020).

References

1 INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State’s Nuclear Security Regime, IAEA NSS No. 20 (2013).

State

Indonesia
Gender

Male

Primary authors:  Mr SIHANA, Sihana (Universitas Gadjah Mada);  Mr PUTERO, Susetyo Hario (Universitas Gadjah Mada);  Mr FERDIANSJAH, Ferdiansjah (Universitas Gadjah Mada);  Mr HAWI-BOWO, Singgih (Universitas Gadjah Mada)

Presenter:  Mr SIHANA, Sihana (Universitas Gadjah Mada)

Track Classification:  CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
Understanding Physical Protection Obligations During International Maritime Nuclear Shipments - the Entry into Force of the CPPNM Amendment

International maritime shipments of nuclear materials are a key enabler to the civil nuclear fuel cycle and the generation of sustainable and carbon free electricity in a number of countries worldwide. In addition to the stringent safety and environmental requirements that exist, these international shipments are required to comply with a range of nuclear security regulations that are applied according to the location and/or flag state of the vessel concerned. The entry into force of the Amendment to the Convention on the Physical Protection of Nuclear Material (CPPNM) in May 2017 marked a milestone in the global effort to strengthen nuclear security. Quite rightly, much attention has focused on the significant broadening of scope of the original Convention with regard to the protection of nuclear facilities and nuclear material in peaceful domestic use, storage and transport. Indeed, the CPPNM Amendment provides for a new "core" undertaking by each State Party to establish, implement and maintain a physical protection regime applicable to nuclear material (and facilities) under its jurisdiction. In implementing this undertaking, the State Party shall: establish and maintain an appropriate legislative and regulatory framework for physical protection; establish or designate a competent authority responsible for its implementation; and take other appropriate administrative measures necessary for the physical protection of such material (and facilities). In this context, the State Party shall (without prejudice to any other provisions of the amended Convention) “apply insofar as is reasonable and practicable” twelve "Fundamental Principles of Physical Protection of Nuclear Material and Nuclear Facilities". In light of these and other changes, this paper considers the impact on the obligations of concerned States Parties (exporting, importing, transit and flag) for international maritime nuclear shipments. In doing so, Part 1 will assess what new or additional obligations have been placed on the concerned States Parties, particularly, flag states, following the entry into force of the CPPNM Amendment. Thereafter, Part 2 describes which state(s) has legal jurisdiction during such shipments. Finally, Part 3 explores any potential gaps or challenges in implementation, with a particular focus on how these could flow down into the sector and its supply chain.

State
United Kingdom

Gender
Male

Primary author: WHITTARD, Ben (International Nuclear Services Ltd)
Presenter: WHITTARD, Ben (International Nuclear Services Ltd)

Track Classification: PP: Transport of nuclear and other radioactive material: practices, challenges and regulatory issues
ENHANCING OF THE YOGYAKARTA NUCLEAR FACILITIES SAFETY AND SECURITY SYSTEM, BY IMPLEMENTING THE SIRESS DIGITAL APPLICATION

Every activity related to the utilization of nuclear power must pay attention to the security, peace, welfare, safety and health of workers and community members, as well as protection of the environment. Further provisions relating to safety and security are regulated in Indonesian Government Regulation (GR) No. 33 of 2007 concerning Safety of Ionizing Radiation and Security of Radioactive Sources and Government Regulation No. 54 of 2012 concerning Safety and Security of Nuclear Installations. The nuclear power regulatory agency also issued a regulation head of Indonesian Regulatory body (BAPETEN) No. 1 of 2009 concerning the provisions of a physical protection system, which regulates the physical protection of nuclear facilities.

The Center for Accelerator Science and Technology (PSTA) as one of the work units at the National Nuclear Energy Agency (BATAN) has the main tasks and functions of research and development in the field of particle physics, process technology and research reactor utilization. As a nuclear center in Yogyakarta, every year PSTA is visited by more than 2000 people to conduct research or conduct study visits and other services. Guests who visit PSTA come from all over Indonesia and even from abroad, such as experts from the IAEA. The large number of visitors who come to PSTA has the potential to become a security threat if it is not managed properly. In order to improve the security level of nuclear facilities, a digital application has been built to register guests online. The project entitled "Register Safety and Security Information System (SIRESS)" is an important breakthrough in order to improve the safety and security of nuclear facilities as one of the vital objects that must be safeguarded for safety and security from the past. This SIRESS application is also a demand of the industrial revolution, which utilizes information technology in facilitating and streamlining the resources of both funds and humans. In terms of security, all visitors can register online from anywhere and at any time. All visitor data is digitally managed, so it’s easy to track. Guests or visitors who will come to PSTA can first register online through the SIRESS application on a smartphone or on a portable computer. Visitors register by filling in the personal data needed and also photos. Visitors who have registered online will get a QR code, and will be validated by security officers when they come to PSTA. Safety side tie, the SIRESS application also provides tests on work safety and radiation protection for students or students who conduct research at PSTA. This test is intended to measure students’ understanding of occupational safety and radiation protection. With the SIRESS application it is expected that the safety and security of PSTA nuclear facilities can be further improved.

State

Indonesia

Gender

Male
Primary author: Mr WIJAYA, Gede Sutresna (PSTA-BATAN)

Co-authors: Mr TRIATMOKO, Isman Mulyadi (STTN-BATAN); Mr JAUHARI, Rahmat (PSTA-BATAN)

Presenter: Mr WIJAYA, Gede Sutresna (PSTA-BATAN)

Track Classification: PP: International Physical Protection Advisory Service: good practices and lessons learned
Approach for Harmony of 3S (Safety, Security and Safeguards) in Japan

In order to secure public safety with utilization of nuclear fuel material, etc., it’s important to avoid mutual bad influence of 3S (safety, security and safeguards) as well as take appropriate measures.

About the harmony of the safety and the security, "INSAG-24 (The Interface between Safety and Security at Nuclear Power Plants)” (2010, IAEA) proposed the important point to integrate safety and security.

“Safety Culture Policy Statement” (2011, NRC) emphasized the importance of reconciling safety and security, and indicated characteristics of the comprehensive safety culture.

IAEA, etc. are considering the harmony of safety and security continually.

In the G8 Hokkaido Toyako Summit (2008), based on the situation that the number of country considered new installation and expansion of nuclear power generation are increasing, the agreement to make 3S the foundation to introduce nuclear power generation that was suggested by Japan was adopted as the international initiative.

In those days, in Japan, it was difficult to plan for the harmony of these regulation because plural government offices had jurisdiction over safety and security regulation separately.

But at the present time, Nuclear Regulation Authority (NRA: established in September 2012) has jurisdiction over nuclear regulation including 3S unitarily.

NRA showed the code of conduct to make an effort toward the harmony of the measure of safety and security in the "NRA’s code of conduct for nuclear security culture" (January 2015) and "NRA’s declaration for nuclear safety culture” (May 2015).

Based on occurrence of following cases including mutual interference, NRA is working on harmony of 3S (not only safety and security, but also safeguards).

- The example that the measure for safety interfere with security is that the measure which the ground of the peripheral protected area is plastered by mortar for a fire protection connects in the state which tends to get over a barrier in the border of the peripheral protected area.
- Conversely, the example that the measure for security interfere with safety is that replacement of a door of the central control room for making sure of delayed performance has an influence on the shielding performance and earthquake resisting, etc. of the central control room.
- The example that the measure for safeguards interfere with safety is that the fire an inspection monitor has caused has an influence on safety in facilities.
- Conversely, the example that the measure for safety interfere with safeguards is that the aseismic reinforcing work in the facilities causes visual field defect of inspection monitor.
- On the other hand, the example that the measure for security interfere with safeguards is that licensee can’t give the photograph filmed by IAEA inspector because the PP information is included in this photograph.

While the interface of 2S (safety and security) is mainly considered internationally, the harmony of the 3S that NRA promotes is a characteristic approach.

For the harmony of the 3S, NRA is promoting the following approach.

- NRA made licensees recognize that licensee has the principal responsibility which plans for the harmony of the 3S and suggested correspondence to licensees.
- To make sure that the staff of safety section can treat PP information and the staffs of safety and security section cooperate efficiently in examination and inspection, the system for confirming personal reliability regarding NRA staff was introduced.
- When licensee submits authorization application about any one of 3S measure, the charge section of this application makes information sharing with other section of 3S and tries to exclude bad influence as much as possible.
- When an inspector notices about other measure among inspecting any one of 3S measure, the inspector informs the charge section of the noticed measure.
- By adding security cases into the emergency division of nuclear hazard, unifying the information communication system in emergency and participation of the staff of safety section to PP training, NRA planned for unification of safety and security in emergency correspondence.
- NRA carries out the combined training with all related organizations (prime minister’s official residence, the police and the Maritime Safety Agency, etc.) as for PP training.
- NRA inspectors will take basic training in all fields as a compulsory subject without selecting safety and security.

**State**

Japan

**Gender**

Male

**Primary author:** Mr OKU, Hirotaka (Nuclear Regulation Authority (NRA))

**Presenter:** Mr OKU, Hirotaka (Nuclear Regulation Authority (NRA))

**Track Classification:** CC: Nuclear safety and security interfaces
Education, Knowledge, Competence - Fundamental Prerequisites for Nuclear Security

Successful implementation of international norms on nuclear security requires a number of prerequisites at the State – including the provision of adequate legal, institutional, financial, technical and human resources. Among the latter (HR), it is often taken for granted that necessary knowledge and competence do exist per se. However, this is not always the case, just the contrary – time, efforts and resources are frequently wasted because these HR fundamentals are not set solid at first.

Education and training are paramount in building knowledge and competence. It is crucial to recognize the importance of formal education, primarily at universities. IAEA based international nuclear security education network (INSEN), even not so long in existence, proved pivotal in the field. Standardization of educational programmes and thoughtfully conceived development of textbooks/literature on key NS subjects turned out to be highly appreciated in Member States. Especially small, developing, non-nuclear countries, starting their NS education from the scratch, are profiting from the network. Education at universities, preferably following INSEN guidelines, is thus fundamental for HR development in NS.

Training is another aspect of HRD, equally important – however quite different in nature from education. Another international network (Nuclear Security Support Centres – NSSC) deals, inter alia, with training aspects of competence.

While education basically stands for knowledge, training contributes to its practical applicability – both being essential constituents of competence. For competence to be complete, one should also include experience and ethics.

Training cannot replace education – attempting so, one falls into a typical competence pitfall. Training is thus meaningful only when superposed onto an adequate education. Messing up these terms will lead to a false perception of knowledge and competence (quasi-knowledge and quasi-competence); eventually, security will inevitably be compromised.

The same is valid for experience – although always welcome and respected, experience cannot replace neither education, nor training, not to speak both of them. Only on the top of the two, experience makes sense and gives a fine touch of maturity to competence.

Ethics is perhaps the least questioned among competence ingredients – it is also often taken for granted. Without going into elaboration, it is enough to think of a knowledgeable, trained, experienced and malevolent person at a responsible position somewhere in nuclear sector – a serious security issue per definition.

Quasi-knowledge and quasi-competence are more perilous for NS than ignorance and incompetence (i.e. clear lack of knowledge and competence), because the latter are more explicit and easier to recognize/prevent/rectify. It is important to note that quasi-knowledge and quasi-competence can be traced behind nearly all nuclear mishaps – from minor/benign incidents (like just clumsy handling of some situations in nuclear community, e.g. poor communication with public/media), to major accidents with grave consequences.

All aspects of competence should thus be properly addressed – education, training, experience and ethics – with adequate place and emphasis for each.

Briefly: there are very few things which can contribute so beneficially to security like knowledge and competence; there are even less of those which can cause so much harm as the false perception of them.
State
Montenegro

Gender
Male

Primary author: Prof. JOVANOVIC, Slobodan (University of Montenegro, Centre for Nuclear Competence and Knowledge Management)

Presenter: Prof. JOVANOVIC, Slobodan (University of Montenegro, Centre for Nuclear Competence and Knowledge Management)

Track Classification: CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
The benefit in Developing and Implementing Instructor Training for Front Line Officer on Nuclear Security Detection in Malaysia

Malaysia has developed nuclear security detection capability focusing at our major point of entries and exits since 2007. The roles of nuclear security detection has been extended thus since then to nuclear security detection for major public event such as to the South East Asian (SEA) Games and Visits of Senior Foreign Leaders as well as to address interior detection on day to day operation in Malaysia. From day one of our experience in developing detection capability, the most challenging observation made was on how to build and ensure continuous capacity for frontline agencies in ensuring their capabilities to perform task related to nuclear security detection. The fact that nuclear by itself is a foreign subject to many, including frontline officer (FLO) agency, has making continuous availability of competent FLO to perform nuclear security detection task is almost impossible. The nature of FLO duties that are subject to job rotational policy has worsened the efforts to sustain nuclear security detection capability within FLO agencies a stumbling block to sustainable initiatives. High ratio gaps between strength of FLO agencies versus the technical competent authorities as the subject matter expert such as regulatory body like the Atomic Energy Licensing Board (AELB) in Malaysia, has pushes us further in finding a sustainable and better strategy to address this matter. The AELB with the support from the International Atomic Energy Agency (IAEA) through Malaysia’s Nuclear Security Support Centre (NSSC) and the United States Nuclear Smuggling Deterrence and Detection (US NSDD) work together in reforming approach to upgrade Instructor Training programme for FLO using a proper Strategic Approach to Training (SAT) methodology. Such approach involved task analysis, revision of FLO training materials, performing training programme, conducting examination and preparing evaluation report to ensure consistency and standard of the trained instructor. Malaysia’s NSSC has piloted the first two (2) weeks course of FLO Instructor Training programme involving 15 participants from AELB, Royal Malaysia Police (RMP) and Royal Malaysian Customs (RMC) in May 2017. Result from the training had produced a new batch of qualified instructor developed through a well-defined programme in ensuring the standard of our FLO training programme. The pilot Instructor course focussed more on hands-on approach in compared to classroom training that does not suit best to FLO’s nature of work. Post the pilot course, the RMP and RMC respectively continue in developing the similar training programme within their organization to produce more trainers and in-house subject matter expert in nuclear security detection. Such approach lessens the dependency of FLO agencies to AELB in delivering training hence providing more opportunity for AELB to analyse and making continuous improvement to the training programme and other technical areas of nuclear security detection. The FLO training was also introduced as one-week Regional Training Course in Malaysia followed by revision of training material with US NSDD to finally come with the end-product that suits the needs of FLO in Malaysia. The trained Instructor were also invited to contribute to IAEA similar training programme in other countries. This strategic approach in implementing Instructors training programme addresses high needs of competent FLO within job rotational environment and has been one of the best initiatives undertaken by Malaysia’s NSSC in the effort to ensure effective and sustainable nuclear security detection capabilities in Malaysia.
Gender

Female

Primary author:  Ms RABANI, Nor Faezah

Co-author:  BAKRI, Noor Fitriah (Atomic Energy Licensing Board (AELB))

Presenter:  Ms RABANI, Nor Faezah

Track Classification:  CC: Role of Nuclear Security Support Centers to support and sustain national nuclear security regimes
Specific Aspect of Physical Protection System Development for Nuclear Facility: Russian experience and lessons learned from international assistance and support activities

Physical Protection System (PPS) is intended to counteract sabotage of nuclear material and nuclear facilities as well as theft prevention of nuclear material. According to Convention on the Physical Protection of Nuclear Material and Nuclear Facilities (including the 2005 Amendment) the State is responsible for development, maintenance and supporting of physical protection regime in its territories, and physical protection (including PPS development) at nuclear facility. The intergovernmental agreements are based on these guidelines and signed on behalf of the Russian Federation with foreign states for cooperation in the field nuclear energy use.

Along with development of nuclear facility, the Russian party can provide the foreign customer with consulting services in the field of PPS development and technical support and assistance in PPS design and equipment installation for nuclear facilities.

NIKIRET is Russian company specialized in PPS design and construction for Russian as well as for foreign customer. Based on its experience and lessons learned from international and domestic assistance and support activities, NIKIRET has developed a basic proposal for PPS development. This basic proposal is applicable for "high power NPP", "low power NPP" and "Nuclear Science and Technology Center". The proposal of NIKIRET is based on:
• the fundamental principles of the Convention on the Physical Protection of Nuclear Material and Nuclear Facilities (including the 2005 Amendment),
• general IAEA nuclear security recommendations.

At the same time, if interested State or customer has additional requirements for PPS, the NIKIRET basic proposal can be tailored accordingly. Taking into account broad Russian experience in physical protection of various nuclear materials and facilities, NIKIRET is able to design PPS of any complexity.

Process of PPS development for foreign countries typically consists of five stages. Russian party can provide assistance and support in four of them:
1) pre-project analysis and development of justifications;
2) PPS design;
3) building and assembling, start-up and adjustment works;
4) assistance in PPS operation;
5) PPS use (sole responsibility of foreign customer).

The proposal of NIKIRET on PPS development consists of two parts – technical (technical security equipment complex) and documentary one (facility-based documents necessary for PPS operation as a whole). The documentary part includes such documents as "Design basis threat", "Vulnerability analysis", "Identification of secured zones", "Conceptual solutions of PPS development", "Technical specifications of PPS development", "Plan for physical protection of nuclear material and nuclear facility during storage, use and transportation across the territory of nuclear facility", "Design documentation". The technical part is implemented through the delivery of full range of equipment and material (from technical security equipment to physical barriers), building and assembling, start-up and adjustment works, according to design documentation for PPS.
State

Russian Federation

Gender

Male

Primary author: Mr SOLOVEV, Aleksandr (NIKIRET – branch of JSC "FSPC "PC "Start" named after M.V. Protsenko Russian Federation)

Presenters: Mr SOLOVEV, Aleksandr (NIKIRET – branch of JSC "FSPC "PC "Start" named after M.V. Protsenko Russian Federation); KHARLAMOV, Vadim

Track Classification: PP: Physical protection systems: evaluation and assessment
DESIGNING NUCLEAR SECURITY CAPABILITIES IN MALAYSIA: ROLE OF NUCLEAR SECURITY SUPPORT CENTRE

The global never ending drive to progress in competing technology development has significantly showed rising numbers in import exports industry, while knowledge transfer and information sharing are now enabled by a finger swipe. Being geographically located in South East Asia, Malaysia shares land borders with Thailand, Brunei Darussalam and Indonesia, with wide part of the west coast of the peninsular is directly facing Straits of Malacca, one of the most important shipping lanes in the world. Driven by this economic, society and environmental urges, building and empowering national capacity to look out for nuclear security matters has been identified as one of the matter in hands for this paper. Since early 1980s, Malaysia has identify the essential needs to be able to have optimum regulatory and controlling capacity of radioactive and nuclear materials available in the whole country. The challenges to really achieve the goal lies on the integrating and coordinating critical stakeholders and their genuine roles. Through Malaysia’s Integrated Nuclear Security Support Plan (INSSP) and the establishment of Nuclear Security Support Centre (NSSC) in 2009 that was spearheaded by AELB, various government agencies started to look at nuclear security issues from their own respective point of view, but in the same direction. Malaysian NSSC offers best practices and information sharing that benefit across the nation. A few structured and carefully tailored programs has been developed and implemented to meet the needs of industrial licensees, with some encouraging and optimistic feedbacks. The unique role of National Security Council (NSC) for nuclear security responsibilities has been introduced in a subtle approach. The fact that the NSC is reporting directly to the Prime Minister Office has delicately emphasize the intensity of authority the council has when delivering orders and delegating responsibilities to other relevant agencies. Bilateral cooperation with neighboring countries has also made possible through the NSSC network and IAEA assistance. A few cross border and maritime exercises has not only upgrade and integrate the existing Standard Operation Procedure (SOP) to handle nuclear and radioactive material out of regulatory control that implicate different countries law enforcement agencies, but has further benefit every party involved with the enhancement of networking between them. The design on this responsibilities sharing have significant implications for strengthening national capabilities in nuclear security concerns to protect and maintain this small country sovereign rights. This paper provide observation on experiences, challenges and good practices of Malaysia’s NSSC with regional roles after 10 years of its establishment. The observations covers planning, implementation and way forward in ensuring sustainable nuclear security capabilities in Malaysia.

State
Malaysia

Gender
Female
Primary author:  Ms MOKHTAR, DEWISINTA (AELB MALAYSIA)

Co-author:  Ms BAKRI, NOOR FITRIAH (AELB MALAYSIA)

Presenter:  Ms MOKHTAR, DEWISINTA (AELB MALAYSIA)

Track Classification:  CC: Role of Nuclear Security Support Centers to support and sustain national nuclear security regimes
Role of Investigation and Legal Prosecutions in Nuclear Security

Malaysia has transparently reported 22 cases of material out of regulatory control (MORC) since 2007 to the International Atomic Energy Agency (IAEA), Incident Trafficking Database (ITDB). Records of data, has shown 14 cases of MORC were reported occurred at the border while the remaining eight (8) cases took place within the interior of the state. In most of border detection cases, the materials were instructed to be sent back to country of origin due to multipipe technical reasons such as lack of legal evidence to support further legal actions and the urgent need to make decision as to avoid impediment to trade including the availability of insurance coverage to support the embargo of the goods. Though half of the problem solved when the MORC were being shipped out formally from Malaysia, there is still a growing concern on what will happened next to the embargoed MORC. The Atomic Energy Licensing Board (AELB) as national regulatory body responsible for controlling the authorised dealing of nuclear and other radioactive materials in Malaysia, with the cooperation of Royal Malaysian Customs Department (RMCD) strived hard in ensuring every trace of evidence will be cautiously handled as to ensure detection cases can be pursued further towards proper legal actions. This is important as to have proper information and gathering of evidences in analysing trend and pattern of every detection cases that will contribute in building risk management for nuclear security detection in Malaysia. After more than 10 years of experience in border detection, this year marked the first experience that we had successfully able to bring the importer to court for further legal action where the importer was instructed to pay the fine of the committed offences. The legal actions have consequences beyond financial implication that is linked to business reputation that would want to be avoided by business entity. Hence, legal action will be the first priority in mind in dealing with any detection cases in Malaysia. In other example, for interior detection, we have also seen the experienced in using a suitable legal provision through cessation of activities against company that committed offences that has resulted in managements awareness in nuclear security compliance due to implication that seems to tarnishing business reputation including loss of business opportunity during the period of offences. Through these observations, Malaysia believe that the holistic approach in nuclear security shall include the strengthening of investigation and prosecution elements in supporting other technical mechanism. Such measures highlight the effectiveness regulatory control for radioactive and nuclear material from nuclear security point of view.

State

Malaysia

Gender

Female

Primary authors:  KOSTOR, MONALIJA (Atomic Energy Licensing Board); BAKRI, Noor Fitriah (Atomic Energy Licensing Board (AELB))
Presenter: KOSTOR, MONALIJA (Atomic Energy Licensing Board)

Track Classification: CC: Implementation of national legislative and regulatory frameworks, and international instruments
PHYSICAL PROTECTION OF SPENT RADIOACTIVE SOURCES

A. Chilulu

a Radiation Protection Authority (RPA), P.O Box 50002, Lusaka
Email address: abigailsimwina2016@gmail.com

SYNOPSIS

In an effort to further enhance the physical protection of spent radiological materials stored in the Radiation Waste Storage Building (RWSB), an agreement was signed by ZCCM-Investments Holding through the Ministry of Health (MoH) and Radiation Protection Authority (RPA) with the Office of Radiological Security (ORS) of United States of America (USA) to design a reliable security system. The agreement was signed in the year 2014.

The agreement between ZCCM-IH and ORS was necessitated by the fact that ORS has a mission to protect and reduce access to vulnerable nuclear and radiological materials located at civilian sites worldwide. Through ORS, physical protection controls were upgraded in order to secure spent sources stored at the interim RWSB.

In line with ORS’s mission, Zambian institutions tasked to protect these materials have continued to take necessary measures to ensure that high priority spent radiological materials are well protected from theft and sabotage. One such measure was the construction of a new guard room for security personnel who monitor and keep surveillance of the spent sources on a 24 hours daily routine. The introduction of this physical protection has greatly improved the security of spent sources at RWSB. The design of the physical protection system is based on the principle of ‘delaying the adversary’ through the presence of physical barriers and security locks.

The early warning systems provided by alarms are further applied to deter unauthorised access to the premises. In addition personnel identification devices in form of proximity cards and biometric fingerprint detectors are used to ensure that only authorised personnel have access to the building.

The Alarm system is arranged in such a way that it has a control panel which codifies signals from detection devices, fixed duress buttons or the system itself and transfers it to a remote central monitoring station.

In addition to the physical barriers and alarm system, surveillance cameras in form of closed circuit television security system (CCTV) with five (5) cameras have been installed. The cameras are positioned in strategic position in order to have a wider view of areas inside and around the premises as follows:

• Outside main entrance area, to view entrance and exit from the RWSB
• Outside back area, covering the entire rear of the RWSB
• Inside RWSB outside grating area looking at the folk lifter and entrance
• Inside RWSB – inside of the grating area left looking at the spent sources
• Inside RWSB – inside of grating area right looking at the spent sources

All security equipment is connected to UPS units to ensure uninterrupted power supply and is also protected against lightning and power surges. There are four (4) UPS units in the RWSB, two (2) on each side of the grating to service the remote panel and the main panel. In addition to this solar panels have also been installed to solve the problem of electricity outages.

The sequence of action is such that, in case of an emergency, the first security element reports the incident to all guard stations to support the site and take control of the situation; however in
circumstances where it is impossible to take control of the situation, first responders have to call a local police station and consequently inform the radiation specialist, who will in turn inform RPA accordingly.

Key Words: Spent Sources, Protection and security

State
Zambia

Gender
Female

Primary author: Ms CHILULU, ABIGAIL (RADIATION PROTECTION AUTHORITY)

Presenter: Ms CHILULU, ABIGAIL (RADIATION PROTECTION AUTHORITY)

Track Classification: PP: Physical protection systems: evaluation and assessment
The integrated Safety-Security training of inspector in Switzerland

Inspections is an important tool of the regulator or supervisory authority to verify that a licensee complies with the applicable laws and regulations. In inspections, the actual state is recorded in a systematic manner and compared with the nominal state. It is therefore obvious that the training of inspectors should also take place systematically.

Inspectors in the field of nuclear security can benefit from the experience of nuclear safety. In Switzerland, the training of inspectors in the nuclear field happens in an integrated manner, namely nuclear safety and nuclear security together. It takes place on-the-job and lasts typically one year.

The inspection process of the supervisory authority has a recognized accreditation. The training of the future inspectors includes the following steps:

- Training of the legal bases
- Training of the inspection process (planning, preparation, execution, reporting)
- Professional training
- Training of safety culture in the nuclear field (integrated safety and security culture)
- Organization of a nuclear facility
- Radiation protection for self-protection
- Negotiation and interviewing techniques
- Technology of nuclear power plants
- Plant tours and visits of the safety-relevant systems
- Participation in inspections as a silent observer
- Supervised leading of inspections
- Examination inspections

The training concludes after the successful examination inspection with the appointment as an inspector by the director.

Importance for nuclear security

From the point of view of nuclear security, the training together with the future nuclear safety inspectors has many advantages. It has also advantage for nuclear safety – from the scratch, the interfaces, similarities, and differences between nuclear safety and nuclear security are made clear and are addressed. For example, the well-known issue of the confidentiality of information, which always exists in the area of nuclear security, is addressed at an early stage and ways are shown of how to comply with both transparency and confidentiality.

The nuclear security inspectors also gain through integrated training a good and comprehensive understanding of the systems important to safety in a nuclear installation. These systems are the ones that nuclear security is protecting against sabotage, but to which even the nuclear security inspectors rarely have access. This knowledge is important not only for inspections, but also for all other supervisory activities, in particular for assessments and the issuing of permits for plant modifications.
An important aspect is the training of the integrated safety and security culture. It is also important for the supervising authority to consider the sometimes conflicting requirements in the areas of nuclear safety and nuclear security when assessing inspection items.

The other advantages of the joint integrated training are:

- Team inspections with nuclear safety and nuclear security inspectors are possible at any time.
- The training of the negotiation and interview technique promotes the more precise data.
- The different disciplines learn from the scratch to work together. Not only during inspections, but also during the daily business.
- The quality assurance of the inspection reports is carried out according to the same standards.
- The enforcement of deviations also follows the same rules.

**Future improvements**
Inspectors for cyber security (who are normally assigned to nuclear security) particularly have to talk to people who is daily business are nuclear safety (eg. ICS engineers of staff functions). In doing so, they communicate with persons who are not familiar with the mindset of nuclear security, e.g. a malicious act. During training, this problem should be dealt with in more detail.

**State**
Switzerland

**Gender**
Male

**Primary authors:** Mr MATTLI, Hans (Swiss Federal Nuclear Safety Inspectorate ENSI); Mr BRAUN-BARTH, Andreas (Swiss Federal Nuclear Safety Inspectorate ENSI); Mr STAUFFER, Bernard (Swiss Federal Nuclear Safety Inspectorate ENSI)

**Presenter:** Mr MATTLI, Hans (Swiss Federal Nuclear Safety Inspectorate ENSI)

**Track Classification:** CC: National nuclear security inspections: training of inspectors, development of procedures and managing findings
Cyber Security guideline development and inspections - experiences with the "opposite" approach

During inspections, one compares the actual state with a nominal state. This nominal state may be based on national laws, regulatory requirements or guidelines, or international standards. However, in the area of cyber security for nuclear facilities, one often finds itself in a dilemma: missing laws or guidelines. The adaptation of laws is a protracted process, and international standards are not sufficiently precise to use it as a clearly defined nominal state in inspections.

Regarding regulatory guidelines, we observed that many countries are having trouble creating such for nuclear facilities. And after the guidelines were put into force, we observed that they are difficult to apply or are not suitable for inspections.

We had the same problems. Over the years, we started with the drafting of a cyber security guideline, but we didn’t succeed. It changed in 2016 when we started to conduct inspections on cyber security in the nuclear power plants without having a cyber security guideline nor specific legal provision. To make matters worse, neither the supervisory authority nor the nuclear facilities had any experience with inspections in cyber security. However, assessment of cyber security in the NPPs was already done before, but without the use of the inspections.

The first inspection, which was carried out in all nuclear power plants, was a so-called "focus inspection", which was carried out together with the colleagues from electrical engineering and human and organizational factors. As a basis (nominal state) a selection of recommendations from the ISO 27001 and the IAEA NSS 17 were used. All major aspects of cyber security (e. g. policies, protection measures, incident response and mitigation) were examined, however on a rather generic level. The results were inconclusive. On the one hand, this focus inspection allowed us to get a good overview of the cyber security measures at the nuclear power plants. On the other hand, nominal states based on an ISO standard or IAEA guidance are rather difficult to apply. Since the recommendations in these international standards (and this also applies to the NSS 17) have some scope of interpretation, they are easily met. But in nuclear facilities, we usually expect higher standards.

In the following years we carried out further inspections in the nuclear power plants. During this process, the topics to be inspected were narrowed, but we went deeper into the topics. With increasing experience, the nominal state could be better defined, which contributed to the credibility of the evaluations. In addition, we learned what exactly we have to specify in a regulatory guideline.

In 2017, we restarted the drafting of a cyber security guideline for nuclear facilities. It now became apparent that the experiences from the inspections allowed us to formulate the requirements in the guideline clear and precise. The applicability of the requirements for the licensee and the usability as a nominal state for inspections are in our opinion much better.

In short, with learning by doing, we first gained experience with cyber security inspections, which proved to be very helpful during the guideline development. We are convinced that this (unintentionally planned) approach has helped us to create a better cyber security guideline and saved us a subsequent revision of it. It should also be noted that the licensees have gained during this time a certain degree of confidence and are now in a better position to understand the requirements in the new guideline.

And last but not least: with this experience, along with the expert review during an IPPAS mission, we have been able to increase our professional credibility both vis-à-vis the licensees and other state institutions.
State

Switzerland

Gender

Male

Primary authors: Mr STAUFFER, Bernard (Swiss Federal Nuclear Safety Inspectorate ENSI); Mr DEJOZ, Jorge (Swiss Federal Nuclear Safety Inspectorate ENSI); Mr MANCO, Angelo (Swiss Federal Nuclear Safety Inspectorate ENSI); Mr LUZIO, Andrea (Swiss Federal Nuclear Safety Inspectorate ENSI)

Presenter: Mr STAUFFER, Bernard (Swiss Federal Nuclear Safety Inspectorate ENSI)

Track Classification: CC: Information and computer security considerations for nuclear security
Strengthening nuclear security framework and role of the regional, bilateral agreements and IAEA assistance.

Paper covers implemented projects for the purpose of strengthening nuclear security regulatory framework and infrastructure, as well as national legislation.
In this paper, I describe how a regulatory authority in Azerbaijan implement provisions of CPPNM, challenges that we faced, how we overcome them, what was the role of Joint programs, regional agreements, national coordination and support of the IAEA.
It explains how important is coordination and cooperation among states and international organizations, emphasis the importance of international instruments and IAEA recommendations and role of IAEA.
There is also given the description of Projects of Azerbaijan Republic with United Stated of America for strengthening national capabilities, training conducted, further assistance and its implementation process and successful results.
Similar projects can be good example for states looking for international support and cooperation which are starting strengthening their nuclear security capabilities and it shows how bilateral, regional cooperation and Joint activities, as well as IAEA assistance through technical cooperation projects in cooperation with the State helps to build, strengthen and maintain the national capacities for nuclear security.
In summary this paper presents an example of successful cooperation and collaboration with states, as well as with the IAEA and EU for establishment national infrastructure, strengthening national legislation and regulatory framework for nuclear security.

State
Azerbaijan

Gender
Female

Primary author:  Ms HASANOVA, Aysel (State Agency on Nuclear and Radiological Activity Regulation)

Presenter:  Ms HASANOVA, Aysel (State Agency on Nuclear and Radiological Activity Regulation)

Track Classification:  PP: Transport of nuclear and other radioactive material: practices, challenges and regulatory issues
Computer Security Considerations for Nuclear Material Software Development

This paper aims to illustrate how modern information security and best practice software development methodologies are applied to ensure appropriate information protection when storing or processing nuclear material inventory data. The Australian Government maintains a maturity based computer security framework for protecting digital systems and associated information. This is the basis for evaluating products, including web based software solutions, to ensure they are certified and accredited as capable of storing official information. Adapting the framework to ensure considerations for nuclear material information security include design, implementation and on-going risk management activities that will be discussed in this paper. Industry standard software development methods ensure outcomes accurately achieve objectives, those being customer needs, security objectives, legal and compliance requirements, amongst others. Integrating computer security controls into the software development lifecycle ensures risk remediation occurs throughout each stage, and stakeholders understand and have visibility into the levels of risk present when developing and operating a web-based application containing nuclear material inventory data.

In order to successfully address each of these factors and incorporate them into a cohesive process, a hybrid software development lifecycle was adopted. A classic approach was utilised at the beginning and end of each project phase to ensure project governance requirements were satisfied. A design review was also performed at this stage in order to ensure both the stakeholders and project team were in agreement on the deliverable for this phase. The classic methodology was combined with scrum and developer sprints. This was done not only to incorporate stakeholder engagement and feedback, but also guarantee that the outcome for each phase of the project was fit for purpose. Due to this high level of stakeholder engagement, all parties including security, regulators, the legal team and the client were able to ensure that their domain specific requirements were met. This paper will also outline other areas of the development practice, the technical framework used and illustrate how the continuous testing regime was instrumental in the successful delivery of the solution.

State
Australia

Gender
Male

Primary authors: STEVENS, Chris (Mr); Mr BARRY, Adam
Presenters: STEVENS, Chris (Mr); Mr BARRY, Adam

Track Classification: CC: Information and computer security considerations for nuclear security
Lesson Learned from Graded Application of Cyber Security Control on ROK Nuclear Facility

Cyber threats had arisen with the rapid developing of information technology, and infringements of cyber threats are often occurring in national infra-structure, including nuclear facilities. In order to prevent and respond to evolving cyber threats, such as distribution of infectious devices through supply chain, and Ransomware, researches on application with effective cyber security measures are continuing in collaborate with nuclear facilities and research facilities. It is recommended to secure and respond to these cyber threats, licensees are to apply it in the field, read the attack vectors and vulnerabilities, and following protection, detection, identification of technology trends for the corresponding and appropriate cyber security measures.

Under the law and related regulations, licensee of Nuclear Facilities in ROK applies and implements cyber security controls and measures required regulatory standard, KINAC/RS015, cyber regulation standard for computer and information system at nuclear facilities. Various attempts and research approaches are in progress on accounting for application of cyber security measures for effective implementation of regulations and find efficiency of implementing cyber security measures to their digital asset. This synopsis introduces the lesson learned of regulatory implementation on the methodology that applied to ROK nuclear facility.

In practice of APR1400 NPP in ROK, a single plant classified about 2/3 of all systems as Critical System, and more than 60% of the total critical systems are found out to be a digital system. Those number for CS and CDA are not specified due to the information confidence of licensee. Excessive efforts for application of a hundred security measures were required to the licensee and much time has to be spent on regulatory inspection and implementation. Excessive efforts for application of a hundred security measures were required to the licensee and much time has to be spent on regulatory inspection and implementation.

After applying graded application on cyber security controls in the field, the estimated reduction of evaluation process for application of security controls is almost one-third of applying 101 security controls for all CDAs. Moreover, if methodology used for graded application on security control is applied to the reduced size of nuclear facility, such as nuclear fuel cyber facility, nuclear waste facility, it would be supportive to both licensee and regulatory body to focus more onto the specified digital asset and security control, eventually leverage and enhance the cyber security level of the facility.

**State**
Republic of Korea

**Gender**
Female

**Primary author:** LIM, SOOMIN (Researcher)

**Presenter:** LIM, SOOMIN (Researcher)
Track Classification: CC: Use of IAEA and other international guidelines for building national nuclear security regimes
Understanding Nuclear Cyber Security Measures, Risks and Consequences: from Tank Levels to Plant Processes

Monday, 10 February 2020 12:15 (15 minutes)

Cyber security has been object of study since the beginning of the digital era. However, until the 2010 Stuxnet case in the Iran’s enrichment facility at Natanz, most of world’s cyber security concerns were directed to the theft of sensitivity information. Due to its specially designed attributes, Stuxnet is considered the first “weapons grade computer virus”.

After the Natanz attack, digital specialists - and countries - changed their attentions to digital attacks against real world physical systems, most of them aiming sabotage. Therefore, in the last few years, cyber defense exercises and training courses improvised simplified test beds with information technology (IT) and operational technology (OT) equipment. However, due to the complexity of nuclear power plants (NPP), the University of Sao Paulo (USP), under the International Atomic Energy Agency (IAEA) Coordinated Research Project (CRP) Enhancing Computer Security Incident Response at Nuclear Facilities (J02008), has been developing a hardware-in-the-loop (HIL) simulator, the Asherah NPP Simulator (ANS). The ANS allows a better understanding of a cyber-attack facility impact. Besides that, a control room human-machine-interface (HMI) has been developed by the Tsinghua University and integrated with the ANS. This HMI aims to allow training exercises under the operator perspectives. Other institutes, like the Austrian Institute of Technology (AIT) and the University of Magdeburg have been integrating and developing anomaly detection tools using the ANS.

The CRP J02008 coordination led to the definition of three main roles: 1) System Builders; (2 Threat Modelers; and 3) Capability Providing Organizations. USP, AIT and Tsinghua University are system builders. Capability providers and threat modellers organizations are developing threat model/scenario approach for research of test cases to mimic good computer security practices in regulatory regimes.

Many OT simulators use industrial tank liquid level controllers as cyber security training tool. Tank level controllers are common to industries such as energy, oil & gas, chemical and metallurgy. These controllers maintain the level of boilers, condensers or pressurized tanks. They usually work by having a piece of software checking and adjusting the balance between inputs and outputs: digital controllers simulate pumps and valves that maintain the level between predefined values. Therefore, tank level controllers are the tools-of-choice to represent the effects of a cyber-attack in a real world equipment.

However, NPP are complex systems that must be represented by complex simulators. With the massive use of digital technology, NPP are becoming more tightly integrated. Even analogue legacy processes have been including digital systems that needed to be well-suited to cyber security challenges. Therefore, the ANS is the heart of a HIL test bed where real control equipment can be interfaced with the model to determine the consequences of sabotage from the exploitation of vulnerabilities resulting in loss of confidentiality, integrity and availability.

The CRP J02008 research activities are based on the premise that, usually, existing simulators do not survive or provide accurate results of the effects arising from simulated cyber-attacks; are not designed to account for cyber-attacks; do not capture the data needed for intensive computer security forensics and analysis; and they do not allow hardware/software integration for testing purposes. Therefore, preliminary research results suggest that going from tank levels to facility functions the development of computer security measures to prevent and protect against cyber-attacks on this equipment and systems.

REFERENCES


State

Brazil

Gender

Male

Primary authors: Dr BUSQUIM E SILVA, Rodney Aparecido (Brazilian Government); Prof. MARQUES, Ricardo Paulino (University of Sao Paulo); Prof. PIQUEIRA, José Roberto Castilho (University of Sao Paulo); Dr PAUL, Smith (AIT Austrian Institute of Technology GmbH); Mr HEWES, Mitchell (International Atomic Energy Agency); Mr PURVIS, Scott (International Atomic Energy Agency); Prof. LI, Jianghai (Tsinghua University); Dr ALTSCHAFFEL, Robert (Otto-von-Guericke University of Magdeburg)

Presenter: Dr BUSQUIM E SILVA, Rodney Aparecido (Brazilian Government)

Session Classification: IAEA Coordinated Research Programmes for Information and Computer Security

Track Classification: CC: Information and computer security considerations for nuclear security
Virtualization-assisted testing of network security systems for NPPs

Monday, 10 February 2020 12:15 (15 minutes)

Nuclear power plants are complex systems with critical controls and measures implemented by computers and dedicated programmable logic controllers. These end devices are grouped into different security levels and zones and are connected by computer networks forming a complex trust relationship between the entities. The boundaries of the zones are separated by specialized security systems, e.g. gateways, firewalls, network diodes and other security devices. The thorough testing of these security devices before deployment is a crucial task of the IT staff. In this paper we propose a virtualization-based testing solution, where the stability, security and reliability of the tested devices can be measured in realistic scenarios.

In the first part of the paper we briefly introduce the different kinds of virtualization techniques. Virtualization is a technique which enables the operation of several virtual computers (called virtual machines) running on one or on a limited number of physical hosts. After that we present the concept of Infrastructure as Code (IaC). This concept allows us to store and deploy the configuration of any computer or network of computers as code. Using the two techniques together is an efficient way to deploy large scale computer networks on demand. We demonstrate the capabilities of the technique by designing and deploying a simplified version of a nuclear power plant’s security level 4 and 5 systems.

In the second part of the paper, we briefly introduce the concept of defense in depth for the design of the network, in which the systems are separated by distributing them in different layers from lower to higher security requirements and in sub zones, in which diverse controls must be applied to ensure communication and access between systems and at the same time collect the necessary information to detect intrusions. With this information we can take another important step in the direction of defense in depth, which is the early detection of incidents and consequently early response to them, thus protecting the zones and layers of our system.

By applying a list of pre-selected controls from IEC 63096 (Nuclear power plants - Instrumentation and control-systems - Security controls) we evaluate different security solutions with open source software such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), proxies and security incident and event monitoring systems (SIEM). In order to determine the ideal set of solutions to be used on an end device or network infrastructure equipment, we use the realistic network deployed by the technique discussed in the first part of this paper. The work described in this paper is supported by the International Atomic Energy Agency (IAEA) under the collaborative research project CRP-J02008.

State

Hungary

Gender
Primary authors: Dr HOLCZER, Tamás (BME CrySyS); Mr BERMAN, Gustavo (CNEA); Mr DARRICADES, Sebastian Martin (CNEA); Mr GYORGY, Peter (BME CrySyS); Mr LADI, Gergo (BME CrySyS)

Presenter: Dr HOLCZER, Tamás (BME CrySyS)

Session Classification: IAEA Coordinated Research Programmes for Information and Computer Security

Track Classification: CC: Information and computer security considerations for nuclear security
Control and monitoring of uranium production in Niger from 1971 to 2018, challenges and opportunities.

CN-278; EVT 1900138
Synopsis
Name: GARBA BARKE HASSANE
Profession: Mining Engineer
Employer: Ministry of Mines
Title: Control and monitoring of uranium production in Niger from 1971 to 2018, challenges and opportunities.
The issues of nuclear materials become major problems around the world due to the expansion of criminality acts and terrorism. Therefore, great concerns have been taken for the protection of these materials. For this, Niger Government, as producer of yellow cake has set up some laws and regulations which are monitoring and controlled by the Ministry of Mines and other related Institutions such as the National Authority of Nuclear Energy (HANEA), the National Agency of Nuclear Security (ARSN), the National Center of Radioprotection (CNRP) etc. Through this coordination, the division of Mining exploitation in which I work, conducts the followings activities: the control and monitoring of laws and regulations, the control and monitoring of uranium production and the protection of nuclear materials. The control and monitoring of uranium production in Niger starts from Feasibility stages of mines up to the transport of yellow cake out of the Country. For this, each mining company must follow mining regulations in force and conventional provisions that bind it to the State. In the process of the control and monitoring of uranium production, my division perform activities such as: the reception and analysis of monthly activities report, the supervision of mining activities each three months, the control and monitoring of uranium exported out of the Country, etc. The storage and transport of yellow cake are done in Niger under strict application of laws, rules and regulations in accordance to national and international laws and regulations. The aims of these efforts are to achieve and maintain effective nuclear security. These could not be attempted without improving and sustaining national nuclear security. Therefore, it is important to know how to secure nuclear materials and how to react when it is out of regulatory control. For this, it is important to learn about” The Control and monitoring of uranium production in Niger from 1971 to 2018, challenges and opportunities”, presentation which will be focused on laws, rules, regulations, experiences learned, challenges and opportunities after forty years of experiences in uranium production. The objective of my participation is to share my Country experiences and learn about other participants to strengthening efforts together.

State
Niger

Gender
Male

May 9, 2020
Primary author: Mr GARBA BARKE, HASSANE (Government Employer)
Presenter: Mr GARBA BARKE, HASSANE (Government Employer)

Track Classification: PP: Nuclear material accounting and control
Small modular reactor: approaches to physical protection provision

SMRs are newer generation reactors designed to generate electric power up to 300 MW, which components and systems can be shop fabricated and then transported as modules to the sites for installation as demand arises.

There is increasing interest in small modular reactors (SMRs) and their applications. Many SMRs are envisioned for niche electricity or energy markets where large reactors would not be viable. SMRs could fulfill the need for flexible power generation for a wider range of users and applications, including replacing aging fossil power plants, providing cogeneration for developing countries with small electricity grids, remote and off grid areas, and enabling hybrid nuclear/renewables energy systems.

Currently, there are more than 50 SMR designs under development for different applications. According to the IAEA document ADVANCES IN SMALL MODULAR REACTOR TECHNOLOGY DEVELOPMENTS, there are three groups of SMR:

- land based
- marine based
- other/mobile (only project).

Despite a small amount of nuclear material used in small modular reactors, it surely needs the organization of the relevant measures of physical protection provision. Let the author briefly analyze the applicability of approaches to physical protection organization, which are described in the IAEA documents of NS series, for each SMR type.

Land based small modular reactors: Russian specialists argue that the approaches to organizing physical protection of nuclear materials, which are given in the IAEA document NSS-13, are fully and completely applicable to this type of reactors. There is no fundamental difference from the organization of physical protection of reactors with the power of up to 300 MW and over 300 MW. The essential parameter is the category of nuclear material, on the basis of which, pursuant to NSS-13, a particular set of physical protection measures needs to be applied.

Marine based small modular reactors etc.:

- platform construction;
- power unit (unfuelled reactor) installation;
- transportation to the deployment site;
- fuel loading;
- operation.

It should be noted that stages 3 and 4 may be swapped around.

In terms of physical protection, transportable SMR concepts (Transportable and/or Floating Nuclear Power Plants (TNPPs and FNPPs respectively)) are not “traditional” nuclear facilities but are considered nuclear facilities when stationary.

If the fuel is loaded prior to the unit transportation to the operation site, its physical protection should be provided in accordance with NSS-13 and also at the operation site.

During the transportation process (either as a part of the unit of separately from in), the physical protection of nuclear materials must be provided in accordance with the Security of Nuclear Material in Transport; NSS26-G.
The methodology of design and evaluation of physical protection systems and measures are similar for each type of SMR. Each State and reactor type has its own threats in the area of nuclear security, but the methodology for developing physical protection measures, contingency plans and/or situations requiring emergency response remains the same.

Assuming that SMRs follow recommendations for a nuclear facility when operating and nuclear security guidance for nuclear materials during transportation, we can conclude that the current IAEA nuclear security documents are applicable to SMRs.

Experience in implementing nuclear security in SMRs may lead to modifications to guidance in the future. Therefore, Member States should continue collaboration in technical exchanges regarding design and evaluation for the physical protection of SMRs and IAEA should extend this experience to develop specific guidance on SMRs if needed in the future.

State

Russian Federation

Gender

Male

Primary author: Mr SAVELIEV, Alexander (State Atomic Energy Corporation "Rosatom")

Presenter: Mr SAVELIEV, Alexander (State Atomic Energy Corporation "Rosatom")

Track Classification: PP: Nuclear security of new nuclear technologies (e.g., small modular reactors)
NSSC in Hungary: operating experiences on field of scientific support

Nuclear Security Support and Training Centers (NSSC) has a role in a country to support relevant authorities and other organizations who are responsible for nuclear security to sustain the national nuclear security regime. NSSCs are covering the areas of human resource development, technical support, and scientific support. An NSSC also helps to implement nuclear security culture and enhances national coordination and collaboration among the various competent authorities involved in nuclear security. Although it focuses mainly on national systems, it also has international importance. The NSSC Network of the International Atomic Energy Agency (IAEA) can be a useful platform to identify other Member States with different capabilities and international training activities to help to strengthen nuclear security within a country.

Hungary is operating an NSSC. The leader organization is the Hungarian Atomic Energy Authority (HAEA) which covers mainly the field of regulation and prevention as well as training activates. Several other facilities like Technical Support Organizations (TSO) help the Authority to sustain the national nuclear security system in the country. One of the TSOs is the Hungarian Academy of Sciences Centre for Energy Research (MTA EK) which is responsible mainly for scientific support. This activity is one of the key areas of NSSCs. In general scientific support services for provision of expert advice, analysis, technology testing and evaluation, as well as research and development (R&D) for nuclear security. This type of assistance is needed when a specific scientific challenge arises that is not covered in existing procedures or specialized analytical capabilities and R&D are needed to handle it.

MTA EK is able to assist different authorities and organizations in the field of R&D to nuclear security instrumentation and applications. Besides, technical reachback is also available as remote support on advanced alarm assessment using expert advice, as well as on-site analytical or operational support to response nuclear security events by stakeholders. MTA EK’s mobile capabilities with preparedness service can provide assistance e.g. during radiological crime scene management. Specially trained subject matter experts and comprehensive knowledge on the usage of radiation measuring devices are available. Trained in-filed practice and several SOPs are also existing for on-site activities, like field activities of the Mobile Expert Support Team.

Specific area is the technology testing to help authorities to evaluate the efficiency and sensitivity of the existing detection systems for improvement. MTA EK is also establishing recently a training facility using different scenarios for first responders to train them to be prepared for various nuclear security events.

Besides, MTA EK is operating a centralized national Nuclear Forensics Laboratory which has technical capabilities, expertise and advanced laboratories equipped with various analytical techniques to analyse radioactive evidences. Dedicated storage for evidences and own chain-of-custody system is also available. Following long-term activities (since 1993) of MTA EK in this field the Centre for Energy Research was nominated as a Collaborating Center of the IAEA for nuclear forensics in 2016.

This paper will present HAEA’s and MTA EK’s capabilities in R&D in the field of HRD and scientific support inside the Hungarian NSSC system.
Gender

Not Specified

Primary authors: Ms KOVACS-SZELES, Eva (Hungarian Academy of Sciences Centre for Energy Research (MTA EK)); Mr STEFANKA, Zsolt (Hungarian Atomic Energy Authority)

Presenter: Ms KOVACS-SZELES, Eva (Hungarian Academy of Sciences Centre for Energy Research (MTA EK))

Track Classification: CC: Role of Nuclear Security Support Centers to support and sustain national nuclear security regimes
Nuclear forensics: further development and stability improvement

The establishment and further development of nuclear infrastructure as well as nuclear security regime in the countries, which are commencing the execution of their nuclear power or research program, is accompanied by objective difficulties related to their limited opportunities and competences. Given the IAEA recommendations and approaches, first, clear coordinating mechanisms need to be established and strategic and current tasks and plans of operation of the competent authorities and organizations, either existing or being created, need to be determined.

The general purpose of the state nuclear security regime is protection of individuals, property, society and environment from adverse consequences of the events related to the nuclear security. To achieve this purpose, countries should establish and put into force an effective and proper nuclear security regime and also ensure its operation and stability to prevent, detect and respond to such events. A nuclear security regime covers nuclear and other radioactive materials regardless of whether such materials are under or beyond regulatory control. Each country should ensure the undertaking of prompts and comprehensive measures to detect and, if applicable, recover the lost or stolen nuclear material.

The system of combating illicit trafficking of radioactive materials provisionally includes two main areas: the documentary area, i.e. information and organizational interaction between the competent authorities involved in the process, and the practical one, i.e. direct performance of forensic and other examinations.

An analysis of the events on nuclear forensics, in which Russian specialists have participated, allows to conclude that:
- the model of establishing the documentary area of the system of combating illicit trafficking of radioactive materials is similar in most of the countries, mainly based on the IAEA recommendations and does not require further clarifications;
- it is necessary to support and develop exactly the practical area of the system of combating illicit trafficking of radioactive materials both within a country and on the international platforms.

Since the establishment, support and development of the practical area require the availability of the relevant competences, it is appropriate to pay more attention to it in future, both within a country and in its international activity, by:
- conducting various training sessions and seminars on practical issues;
- practice exchange;
- joint development and improvement of radioactive materials identification techniques;
- dissemination of the techniques among the countries concerned;
- development of training programs;
- carrying out training in various formats;
- strengthening the role of the Global Initiative to Combat Nuclear Terrorism.

A special attention needs to paid to the international cooperation on nuclear forensics issues. Most of the nuclear forensics’ issues are known to be of sensitive nature, so the issues of protection of confidential information and ensuring national security of each country play the key role. That is why further development of international information interaction on nuclear forensics issues should be based, above all, on the national legislation, conclusion of agreements between countries and reliability of the data being transferred.
State

Russian Federation

Gender

Male

Primary author: Mr SAVELIEV, Alexander (State Atomic Energy Corporation "Rosatom")

Presenter: Mr SAVELIEV, Alexander (State Atomic Energy Corporation "Rosatom")

Track Classification: MORC: Nuclear forensics
Nuclear Forensics – Combining Research, Application and Investigation

Nuclear forensics is defined as "Nuclear forensics is the examination of nuclear or other radioactive material, or of evidence that is contaminated with radionuclides, in the context of legal proceedings under international or national law related to nuclear security. The analysis of nuclear or other radioactive material seeks to identify what the materials are, how, when and where the materials were made, and what their intended uses were."

Nuclear forensic science has emerged as a relatively new and fascinating multidisciplinary area of research, combining methods of traditional forensics, radiochemistry, analytical chemistry, material science, isotope geochemistry, and nuclear physics. By providing examples of real incidents, the presentation will illustrate the evolution of this discipline from an ad-hoc analysis to a matured discipline with remarkable capabilities. It should be noted, though, that nuclear forensics first of all provides a comprehensive characterization the material which includes the measurement of isotopic composition, elemental composition, chemical impurities and morphology. These parameters can best be understood by comparing them against data of material of known history. Such an evaluation may either consist in a direct comparison of data (i.e. database query seeking for matching records) or it may consist in point-to-model comparison (i.e. comparing analytical results to model calculations). These findings provide investigative leads to law enforcement or other competent authorities; they might also allow drawing conclusions on the possible origin of the material.

The development or adaptation of analytical methods and the quest for signatures characteristics for the processing history of the material was often inspired by real incidents.

Nuclear forensics is a key element of the response to nuclear security incidents and contributes to deter nuclear proliferation and nuclear terrorism through the wealth of information it may provide on the history of unknown material.

State
- Other

Gender

**Primary authors:** MAYER, Klaus (European Commission - Joint Research Centre, Institute for Transuranium Elements); WALLENIUS, Maria (European Commission, Joint Research Centre, Institute for Transuranium Elements)

**Co-authors:** VARGA, Zsolt (European Commission - Joint Research Centre); RAUFF-NISTHAR, Nadya (European Commission - Joint Research Centre); KRACHLER, Michael (European Commission - Joint Research Centre)

**Presenter:** WALLENIUS, Maria (European Commission, Joint Research Centre, Institute for Transuranium Elements)
Track Classification: MORC: Nuclear forensics
Field test of the C-BORD (effective Container inspection at BORDer control points) project at the land border crossing place in Röszke, Hungary.

The main purpose of the H-2020 C-BORD (“effective Container inspection at BORDer control points”) EU project (2015-2018) was to develop, combine and test new comprehensive and cost-effective detection methods for higher efficiency non-intrusive inspection of freight containers to reduce false negative and positive alarms and to reduce safety risks for customs agents. These technologies are planned to be applied both at sea ports and at land border crossing points to control the illegal trade of e.g. cigarette, drugs, explosives, arms, radioactive and nuclear materials and stowaways. Five different detection methods developed to protect EU borders were trialled at three field tests at sea ports (Rotterdam and Gdansk) and at a land border crossing place at the Hungarian-Serbian non-EU border in Röszke. These detection methods involved (1) an advanced X-ray scanning system, (2) a set of relocatable and mobile radiation portal monitors, (3) a new design of evaporation based detectors, (4) a rapidly relocatable RRTNIS system and (5) the first EU photofission system to detect special nuclear materials. The first three techniques were tested in Hungary at a medium throughput land border crossing point in Röszke.

The next generation cargo X-ray system has been designed to improve both the accuracy and the material classification capabilities of the X-ray images. The new HCVM-T X-ray scanner (of Smiths Detection), capable of operating both in portal and in mobile modes is used to inspect entire trucks, containers and even smaller vehicles for threats such as explosives, narcotics, weapons of mass destruction (WMDs), contraband, as well as for manifest verification, reducing the need for manual inspection. When equipped with the automatic radioactive material detection, the unit simultaneously carries out both the X-ray inspection and an analysis to detect the presence of radioactive gamma and/or neutron materials within the container or vehicle.

The current version of RPMs (of Symetrica and CEA) is a new generation of passive neutron and gamma detection systems used both in mobile and relocatable arrangements, designed to detect radioactive and nuclear materials. The main aim of the passive technology development is to achieve better sensitivity and improved isotope identification. The new design is capable of determining the category of the radioactive material and its position in the cargo. During the field validation exercises two types of RPM systems, integrated with a HCVM-T X-ray system were tested by using various radioactive and NORM materials. Besides this RPM system, similar gamma and neutron detectors were located in a personal car and were used during the field exercise to test both mock-up containers and commercial trucks.

The evaporation based detector system (of Manchester University and Bonn-Rhein-Sieg University) detects volatile chemicals that may be present in a container, giving warning of hazard or contraband. Information given by the EBD is intended to complement X-ray imaging, and/or NII results from other technologies and intelligence by enabling molecular specific detection (i.e. chemical information instead of physical properties). C-BORD implements a new biomimetic approach to detect and identify volatile chemicals within the atmosphere of a container. Thus, the capability to identify a specific target is subject to the volatility of the respective substance and is directly influenced by the packing/sealing of the substance.

In the frame of the field exercise pre-prepared (mock-up) containers/freight trucks were filled with cargo (e.g. paper, clothes, wood) and threat materials (e.g. tobacco, arms, radioactive materials) for the tests. Besides the prepared containers, real containers loaded with commercially traded products were also selected for control by the C-BORD technologies, as part of the regular daily
As a conclusion it was found, that the next generation cargo X-ray system of SmithsD with improved accuracy and material classification capabilities has fulfilled the expectations. Similar conclusions were drawn with respect to the high level performance of the Symmetrica designed mobile, portable, built-in and fixed relocatable monitors. The CEA designed fixed radiation portal monitor has shown also good performance. The gas phase detection technology was evaluated as a promising method, which requires further development and testing.

The idea of combining detection technologies to maximize effectiveness and efficiency was achieved by developing the common user interface, which allows better allocation of human resources and also facilitate to shorten the time of the customs inspections. This is with no doubt one of the biggest benefits of the C-BORD project. Summarizing the test experiences gained at the Röszke land border crossing location from the customs point of view it was found that the present system is simple, easy to operate and the operation does not require serious expertise. It was also concluded, that customs organizations need more technology support for the control of non-commercial traffic and private vehicles.

State

Hungary

Gender

Male

Primary authors:  Mr KOVACS, Andras (Hungarian Academy of Sciences Centre for Energy Research (MTA EK)); Dr VÖLGYESI, Péter (Nuclear Security Department, Hungarian Academy of Sciences, Centre for Energy Research); BODOR, Károly (scientist); Mr BARTHA, András (National Tax and Customs Administration); DANKÓ, Roland (National Tax and Customs Administration); NAGYMIHÁLY, Zoltán (National Tax and Customs Administration)

Presenter:  Mr KOVACS, Andras (Hungarian Academy of Sciences Centre for Energy Research (MTA EK))

Track Classification:  CC: Advances in nuclear security research and development; international cooperation on nuclear security research
Alarm data research of Vehicle Radiation Portal Monitor (RPM)

Carry out various research experiments of Vehicle Radiation Portal Monitor (RPM) by truck which loads fertilizer and nuclear material. The detail content of experiments as follow:

1. Different load of natural radioactive material (fertilizer) experiment.
2. Different activity of nuclear material experiment.
3. Different vehicle speeds experiment.
4. Different loading locations of natural radioactive material (fertilizer) experiment.
5. Natural radioactive material (fertilizer) and nuclear material together load experiment.

According to the test data of these experiments, we can verify the relationship between the weight (activity) and the number of gamma counts of RPM, study the impact of various factors (speed and load location) to the alarm data of RPM and how the nuclear material affect the gamma counts of RPM from the natural radioactive material. Thus we can improve the assessment method of initial alarms from RPM, promote the effectiveness and efficiency of RPM, and ensure to prevent illicit trafficking of nuclear and radioactive material.

State
China

Gender
Male

Primary authors: Mr YANG, changjie; Mr HAN, yeliang; Mr LIU, qi; Mr FAN, suyang

Presenter: Mr YANG, changjie

Track Classification: MORC: Preventing illicit trafficking of nuclear and radioactive material
Detector Applications and Testing Laboratory at the Centre for Energy Research, Hungarian Academy of Sciences (MTA EK)

The Nuclear Security Department (NSD) of the Centre for Energy Research, Hungarian Academy of Sciences (MTA EK) operates a Detector Applications and Testing Laboratory (DATL) in Hungary. MTA EK and the NSD, being the Nuclear Security Support Centre of Hungary together with the Hungarian Atomic Energy Authority, put a great emphasis on applied research work and prototype testing in the field of Nuclear Security applications.

The aim of the DATL is to keep track of, try out, and give expert opinion on the evolving novel technologies which could have a significant impact on the practical applications in Nuclear Security. The expertise of the DATL includes laboratory based and in-field tests of commercial detection equipment, concerning standard compliance testing and suitability testing for a given user application. The standard compliance tests are supported by a wide variety of available industrial, nuclear and NORM materials, and a medical isotope manufacturing company at the same site as the DATL. The suitability testing focuses on the user specific operational and technical requirements of the detection systems, while facilitating discussion with end-users, and hosting field-trials. Prototype testing includes the completion of customized test campaigns in close cooperation with manufacturer companies, providing assistance in preparing for standard compliance tests or tenders.

The applied research work of DATL covers topics from various scientific fields. By investigating the needs of nuclear security stakeholders and the development of technology worldwide, we aim to bring forward new ideas, experiments, and practical implementations of advanced technics and procedures, which would make the operations of the relevant organizations safer and easier. The DATL and the Nuclear Security Department promotes national and international cooperation in research and development, and training areas in Nuclear Security.

State
Hungary

Gender
Male

Primary authors:  Mr VOLGYESI, Peter (Hungarian Academy of Sciences Centre for Energy Research);  Ms CSOME, Csilla (Hungarian Academy of Sciences Centre for Energy Research);  Mr KOVACS, Andras (Hungarian Academy of Sciences Centre for Energy Research (MTA EK));  Mr GULYÁS, Attila (Nuclear Security Department, Hungarian Academy of Sciences, Centre for Energy Research);  Mr TÓTH, Csaba (Nuclear Security Department, Hungarian Academy of Sciences, Centre for Energy Research);  Mr DÓSA, Gergely (Nuclear Security Department, Hungarian Academy of Sciences, Centre for Energy Research);  Mr NAGY, György (Nuclear Security Department, Hungarian Academy of Sciences, Centre for Energy Research)

Presenter:  Mr VOLGYESI, Peter (Hungarian Academy of Sciences Centre for Energy Research)
**Track Classification:** MORC: Building and maintaining nuclear security detection architecture
KUCA Conversion Project - challenges and achievements -

On June 2016, the governments of the United States of America and Japan has agreed to convert Kyoto University Critical Assembly (KUCA), located at Osaka, Japan from highly enriched uranium (HEU) fuel to low enriched uranium (LEU) fuel and to return all HEU fuel materials from KUCA to United States. Based on this mutual agreement, Kyoto University has been working extensively on both the LEU conversion and HEU return of KUCA with close collaboration with USDOE and MEXT and, especially with support from ANL, CERCA and KAERI on the LEU conversion project, which will be focused on this paper.

The Kyoto University Critical Assembly (KUCA) is a multi-core type critical assembly dedicated for the fundamental research and education on reactor physics. KUCA consists of one light-water moderated ("Wet") core and two solid-moderated ("Dry") cores, both currently utilizing highly enriched uranium fuels. Pulsed D-T neutron generator is installed in the reactor building and could be used in combination with one of the solid-moderated core (A-core). 100MeV proton beam from the FFAG proton accelerator complex (installed in adjacent building) together with tungsten or beryllium targets is also available as spallation neutron source in combination with the A-core for fundamental studies on accelerator driven system (ADS). The combination of different core types and neutron sources could be considered as the unique feature of KUCA among the existing critical assemblies in the world.

This LEU conversion project is the first attempt to convert a critical assembly from HEU to LEU. Extensive efforts have been hitherto made to conserve and even extend the capabilities of KUCA experiment after conversion. Preceding the present conversion project, a joint feasibility study on neutronic characteristics of the KUCA LEU cores have been initiated between ANL and Kyoto University, which finally resulted to show the feasibility of converting KUCA with LEU fuel and to preserve the wide variety of neutron spectrum as well as core configuration achievable at the facility. Further investigation in the fuel design resulted to selection of uranium silicide dispersion fuel for Wet core fuel, and uranium molybdenum dispersion fuel for Dry core fuel. The latter posed a significant challenge in coating / cladding technology development to ensure the integrity of the fuel during manipulation for the KUCA operation. Innovative design for Dry core coupon fuel based on "jewelry box" concept has been adopted, which conceals the U7Mo-Al fuel core inside machined aluminum case and aluminum lid fixed by laser welding. Technology development using both surrogate material and depleted U7Mo at CERCA is ongoing.

The Dry core coupon fuel fabrication will be the first experience for UMo based fuel production. In order to facilitate the startup of the fabrication project, KAERI has joined this project as a supplier of the U7Mo atomized powder for industrial production of Dry core coupon fuel; the atomized powder will be fabricated at KAERI using LEU metal supplied by USDOE.

The conversion project is foreseeing the KUCA conversion to be achieved on calendar year 2021. This conversion is expected to be the first critical facility to be converted to LEU and be a significant achievement for nuclear threat reduction and HEU minimization in civilian sector. Moreover, this would be the first critical reactor to be operated by U7Mo based fuel, which shall be providing invaluable scientific data to research reactor conversion community.

State

Japan
Gender

Male

Primary author: Prof. UNESAKI, Hironobu (Institute for Integrated Radiation and Nuclear Science, Kyoto University)

Co-authors: Prof. MISAWA, Tsuyoshi (Institute for Integrated Radiation and Nuclear Science, Kyoto University); Dr TAKAHASHI, Yoshiyuki (Institute for Integrated Radiation and Nuclear Science, Kyoto University); Dr STEPNIK, Bertrand (Framatome-CERCA); Dr ALLENOU, Jerome (CERCA Framatome); Dr RONTARD, Cyrille (Framatome-CERCA); Mr GESLIN, Dominique (Framatome-CERCA); Dr STEVENS, John (ANL); Dr MORMAN, Jim A. (ANL); Dr ALIBERTI, Geraldo (ANL); Dr PARK, Jong Man (KAERI); Ms DICKERSON, Jaci (USDOE); Mr WAUD, Brian (USDOE)

Presenter: Prof. UNESAKI, Hironobu (Institute for Integrated Radiation and Nuclear Science, Kyoto University)

Track Classification: PP: Minimization, on a voluntary basis, of high enriched uranium within civilian stocks and where technically and economically feasible
Human Factor in Nuclear Security

There is no doubt that the Human factor in many industrial activities is highly important. In fact regarding Safety, the Reactor Operators who work in Control Room or even those who are dealing with important safety equipment have a very comprehensive and intensive training to pass very hard and difficult exams to get their license to work. During the last decades the Probabilistic Safety Assessment has focused a great amount of efforts in testing the human errors and studying the human reliability. But those PSA have been focused just only in safety staff.

1. Regarding Security there are several groups of people working in a Nuclear Facility who can be grouped in:
   a. Security operators dealing with Control Alarm Stations functions, Control Access process, Patrolling, etc.
   b. Maintenance Operator of Security Systems, repairing, fixing and caring not only the hardware, also the software.
   c. Security Staff working under the Security Manager who are writing procedures, organizing training and exercises, dealing with the rest of groups, etc.
   d. Response Units who could be inside the facility, as it happen in many countries.

This paper of Human Factor identifies the roles of everyone of those 4 groups who have a direct interaction with the Physical Protection System at the Nuclear Facility.

2. They should have to pass a trustworthiness process before getting the job, a training course about Security Regulation, the knowledge of the Physical Protection Plan and Procedures, their functions and responsibilities in case of contingency, etc. Should there be a minimum requirement in the Regulations for those subjects?

This paper of Human Factor reviews those minimum requirements for those 4 groups that should make evident they get before starting to work in a nuclear facility.

1. They should also perform those functions in exercises to test the security of the Facility and their roles. Is there any comprehensive exercise in which all of them could perform their capabilities? Should it be a requirement? How is in the real life?
   This paper of Human Factor claims about the necessity and obligation of performing partial drills, table tops and comprehensive exercises to test all the security functions and people who have been involved.

2. Who and how is controlling the behavior of those Security 4 groups? Because everyone of them are potential insiders. In just a few of countries there are some kind of Behavioral Observation Programs, but is that enough?
   This paper of Human Factor tries to find some general ways to deal with that subject

State
Spain

Gender
Male
Primary authors: Mr ANTONIO, Perez (Consejo Seguridad Nuclear); CALVIN, Miguel (CONSEJO DE SEGURIDAD NUCLEAR ); LARDIEZ, Pedro (CONSEJO DE SEGURIDAD NUCLEAR )

Presenter: Mr ANTONIO, Perez (Consejo Seguridad Nuclear)

Track Classification: CC: Nuclear security culture in practice with a focus on sustainability
Real-Time Monitoring of Nuclear Cargo Conveyance Using ARG-US TRAVELER

The ARG-US (meaning "Watchful Guardian") TRAVELER has been developed under the auspices of the U.S. Department of Energy (DOE) Packaging Certification Program, Office of Packaging and Transportation, Office of Environmental Management. It is the latest innovative product in the family of ARG-US remote monitoring systems technology for risk-significant materials in cargo conveyances during transportation by truck, rail, or ship. Risk-significant materials may include nuclear and other radioactive material, radiological sources, and/or hazardous chemicals, for which safety, security, and safeguards are major concerns, because the threats of sabotage and theft are real with very serious potential consequences. The TRAVELER’s modular platform, both in hardware device components and software interface drivers, allows sensors to be added or removed (i.e., customized) with relative ease. For example, the TRAVELER’s modular suite of sensors may include temperature, humidity, and radiation (gamma and neutron) sensors, as well as a 3-axis digital accelerometer, an electronic loop seal, and a digital camera, depending on monitoring needs. The TRAVELER also uses redundant methods (i.e., cellular and satellite) for the transmission of sensor data, alarm annunciation when sensor thresholds are violated, and clearance of alarms remotely from a command center, all dynamically with time stamps and GPS locations. Powered by rechargeable lithium-ion batteries, the TRAVELER in its current configurations can support continuous tracking and monitoring (at 2–5-minute intervals) for up to 6 days.

This paper will describe recent demonstrations of the TRAVELER in a rail and a truck shipment of nuclear cargo conveyance in the United States. We will focus on sensor performance, particularly data analytics and alarms annunciation, after preset sensor thresholds are violated in “staged” incidents during transportation and “simulated” in-transit storage. The staged incidents included temperature alarms, as well as alarms caused by disengaging an electronic loop seal and violation of the invisible geofences. We will also discuss the addition of a digital video camera externally to the TRAVELER (via a USB connection) to enable investigation of incidents (and/or accidents) after their occurrence in the field. Future development of the ARG-US TRAVELER system may include (1) addition of dynamic weather maps for the web application user interface; (2) addition of a geographic information system (GIS) to enhance emergency response and enable users to access lists of key resources, including all emergency medical service stations, fire stations, hospitals, local law enforcement, and state emergency operations center within a user-defined region surrounding the incident/accident; and (3) deployment of a self-forming, wireless sensor network (WSN) of TRAVELER and blink sensors by the emergency responders to gain situational awareness near real-time and actionable information in the field.

Reference:
Primary author: Dr LIU, YUNG (Argonne National Laboratory)

Co-authors: Mr CRAIG, Brian (Argonne National Laboratory); Dr SHULER, James (USDOE)

Presenter: Dr LIU, YUNG (Argonne National Laboratory)

Track Classification: PP: Transport of nuclear and other radioactive material: practices, challenges and regulatory issues
Implementation of radioactive source security regulatory infrastructure in electronic licensing of radiation application (eLORA) - an Indian perspective

Introduction:
Ionizing radiation sources are used in multifarious applications in various fields such as medicine, industry agriculture, research, etc. Safety record of the sources used in these practices is generally good, however, if radiation sources are not handled safely and securely then it may give rise to potential exposure leading to unacceptable health hazards including death of exposed person. Regulation of facilities using ionizing radiation in India are carried out by Atomic Energy Regulatory Board (AERB). It is a statutory requirement, in accordance with the Atomic Energy (Radiation Protection) Rules, 2004 issued under Atomic Energy Act 1962, that all the radiation facilities need to obtain requisite License from AERB.

The remarkable growth of Radiation Facilities in India has posed tremendous challenges for AERB to enforce safety regulation at all these facilities effectively and efficiently to ensure safety and security of radiation sources all the time. In order to meet the challenges, AERB took initiative for implementing state of art e-Governance system, eLORA (e-Licensing of Radiation Applications) through automation of regulatory processes associated with the use of ionizing radiation in India.

Key note on the eLORA system:
eLORA is a web-based Information and Communication Technology application establishing direct communication channel between AERB and its stakeholders for exchange of information and communication transaction for delivering its regulatory services as well as for achieving higher efficiency, reliability, traceability and transparency in dealings.

The process developed in eLORA system is as per stipulated requirements of the Atomic Energy (Radiation Protection) Rules, 2004 and regulatory documents developed by AERB (viz. Regulatory Codes, Manuals and Standards). Various modules have been designed, developed and implemented for external stakeholders such as Radiation Facilities, Supplier, Manufacturer, Disposal Agencies etc. and internal stakeholders such as AERB officials operating from head office located at Mumbai and other regional offices located at different parts of the country.

Regulatory Infrastructure implemented for safety and security:
Introduction of each end-user starts with registration process in eLORA wherein various supporting documents for facility and its owner are reviewed. Regulatory infrastructure for ensuring safety regulation have been compartmentalized with various modules. The application forms for various regulatory clearances are interlocked among the subsequent consenting stages such as siting, design, commissioning, etc. and integrated to aforesaid compartments with emphasize on the tracking of radiation sources starting from the procurement to its safe disposal i.e. cradle to grave.

Similarly, regulatory infrastructure for implementing security measures at Radiation Facilities have been considered in eLORA. The module “Security of Radioactive Source” consists of Categorization of sources and detailed security plan submission mechanism. It has been constructed along with various upload provisions catering the need for first submission and subsequent re-submissions/ad-hoc submissions owing to the modification/change in facility layout/design/occupancy, change in functional status of the radiation sources, augmentation of new radiation sources, change in security scenario, increased threat perception etc. System creates interlocks in case of non-availability of qualified security plan while submitting the applications for source procurement,
commissioning and operational licence with a decision making provision at regulators end. As eLORA is an integrated system, provision for submission and review of security plan for medical/industrial practices and during transport are in place. Additionally, provision has been made for submission of Police Verification Certificates of key personnel for Category 1 radiation facilities. Non submission and non-availability of qualified security plan will attract regulatory non-compliance and enforcement actions. Provision has also been designed keeping in view to extend the System for other coordinating government authorities involved in implementing the security measures at radiation facilities.

To facilitate stakeholders for submission of security plan a detailed checklist is provided to ensure that the plan is as per the prescribed security guide of AERB. Security plan is institution-centric irrespective of various practices available at the institute. Accordingly, interdependence across the practices, sharing of resources, and credit from safety systems are part of this Module in eLORA.

During the plan submission process, stakeholders need to declare/provide the operational status of the existing radiation sources/institute, police verification details and all relevant attachments such as security plan, PVC copy, layout of the facility indicating security architectures etc.

An AERB official, identified for this purpose receives the complete submissions. The review process depends on the categorization of the facility. For Category 1 & 2 facilities, security plans are reviewed through a committee and for Category 3, 4 & 5 facilities, security plan are reviewed within the Division as per the stipulated review process. The review comments are recorded and appropriately transmitted through eLORA to the end users regarding the shortcomings/acceptance of the submitted plan.

**Conclusion:**

All of our radiation facilities using radioactive sources are harnessing the benefit of eLORA system. Source categorization feature in eLORA helps in implementation of graded approach in various regulatory functions at the same time compliance towards implementation of security measures has been increased.

**State**

India

**Gender**

Male

**Primary authors:** MISHRA, Bibekananda (Atomic Energy Regulatory Board, Mumbai, India); Dr SEN, Amit (Atomic Energy Regulatory Board); Dr DASH SHARMA, Pankaj Kumar (Atomic Energy Regulatory Board)

**Presenter:** MISHRA, Bibekananda (Atomic Energy Regulatory Board, Mumbai, India)

**Track Classification:** CC: Establishing and formalizing nuclear security processes into integrated management systems
Nuclear safety and security interface: experience of the Russian Federation

Nuclear security aims at protection of people and assets, as well as the environment against the radiological consequences of malicious acts involving nuclear material, other radioactive substances or their associated facilities. Nuclear safety aims at protection of workers, the public and the environment from undue radiation hazards by means of ensuring proper operating conditions, prevention of accidents or mitigation of accident consequences.

While there are many apparent similarities in the areas of nuclear safety and nuclear security, it is important to take into consideration differences which are obvious in the process of documents development, as well as in the process of practical solutions implementation. Nominal merge of nuclear safety and nuclear security into one system is impossible because nature and principles of structure and functioning of the two systems are different, they are based on distinct legal bases, the level of responsibility of a state is not the same, as well as the terminology is diverse.

Nuclear security, as well as nuclear safety, has its main purpose - the protection of people, society and the environment. However, the sources of the threats in these two systems are completely different what dictates the principles and approaches to protection against these risks. For safety assurance, it is necessary to neutralize the risks arising from unintended events (natural occurrences, hardware failures, other internal events or interruptions) or human mistakes; whereas, for nuclear security it is necessary to minimize the risks arising from malicious acts (unauthorized removal and sabotage).

It is important to notice that nuclear security is an area which is based on sensitive information, often classified information (state secret). Approach to achievement of nuclear security objectives significantly differ from approach to achievement of nuclear safety objectives, inter alia because of obligation to information protection. Nuclear security does not allow for the same level of transparency and international obligations, as it is present in the field of nuclear safety. In the area of nuclear security, the IAEA acts only upon a request from the Member States what confirms the specific nature of the area as well.

It is necessary to highlight that interaction of nuclear safety and nuclear security is present constantly. Some elements, actions and documents serve the common purpose of overall protection. Such joint aspects require evaluation and coordination before they are applied. In the Russian Federation on the level of competent authorities and nuclear facilities, approach to interconnection of nuclear safety and nuclear security exists already on the pre-design stage. In the course of vulnerability analysis for a facility during the PPS design, nuclear safety specialists assists in identifying vulnerable parts of nuclear facility which are further protected by physical protection specialists. In addition, further examples of coordination of nuclear safety and nuclear security are as follows:
- development of one evacuation plan;
- design of premises where nuclear materials are located;
- rule of two (three) usage;
- establishment and sustainability of nuclear safety and security culture.

Considering all abovementioned, the following conclusion is reasonable: nuclear safety and nuclear security are independent, connected and mutually reinforcing areas. Concurrently, merging the two systems is unacceptable due to their different nature and characteristics. Interconnection and interface of the systems shall be taken into account in order to reach the common goal. Simultaneously, each of the two systems is equal and autonomous; none shall be subordinating or prevailing to the prejudice of the other.
One of the tasks of the IAEA and countries with significant experience of reliable, safe and secure operation of nuclear facilities and use of nuclear and other radioactive materials is to provide assistance and support upon request to newcomer countries interested in the development of nuclear infrastructure for launching nuclear power or nuclear research programmes. Such assistance and support involve exchange of the relevant experience which at the moment confirms that the approach of independent and coordinated systems - nuclear safety and nuclear security – is effective.

State

Russian Federation

Gender

Female

Primary author:  Mrs AFANASYEVA, Taisiya (State Atomic Energy Corporation "Rosatom")

Presenter:  Mrs AFANASYEVA, Taisiya (State Atomic Energy Corporation "Rosatom")

Track Classification:  CC: Nuclear safety and security interfaces
Integrating Safety and Security by Design for Transportation Packagings of Nuclear and Other Radioactive Material

In a resolution at the International Atomic Energy Agency (IAEA) 2002 General Conference, the IAEA adopted an integrated approach that includes physical protection and material accounting for transport of radioactive material and nuclear material and recommends that security system designers consult with safety experts. In this paper, we present examples of the integration of safety and security by design for two transportation packagings of nuclear and other radioactive material: “smart drum” technology and a new compact Type B packaging design.

The “smart drum” technology, described in reference 2, is the coupling between (1) a robust drum-type transportation packaging that meets all regulatory requirements and safety standards for nuclear and other radioactive material and (2) the ARG-US radio frequency identification (RFID) system with multiple sensors that enables remote tracking and monitoring of the packages in real time, with automatic alert/alarm capabilities, to enhance security during transportation and in-transit storage. The ARG-US—meaning “watchful guardian”—RFID system was developed by Argonne National Laboratory (Argonne) for the U.S. Department of Energy (DOE) Packaging Certification Program, Office of Packing and Transportation, Office of Environmental Management. The system consists of RFID tags, readers, and software for local and web-based applications that can continuously monitor and track tagged packages during storage, processing, transportation, and disposal. Demonstrations and field-testing of the ARG-US RFID systems for drum-type packages during storage and transportation have been conducted at selected DOE sites, including Argonne, Savannah River National Laboratory, and the Nevada National Security Site. Development, testing, and integration of radiation sensors (gamma and neutron), tactile and electronic loop seals, readers and multiple communication platforms, secured servers, and web application user interfaces have also continued over the last ten years. The patented RFID surveillance tag was licensed to Evigia Systems, Inc., in 2014. The system is commercially available and meets U.S. export control requirements.

The other transportation packaging is a new compact Type B packaging design for storage, transport, and disposal of disused radiological sources. Results of engineering analyses showed that the compact Type B packaging design could accommodate up to seven disused CsCl capsules, with a total heat dissipation capability of up to 1,000 W. The all-stainless-steel packaging design provides excellent structural, thermal, and shielding performance under normal conditions of transport (NCT) and hypothetical accident conditions (HAC), as specified in the U.S. Title 10 of Code of Federal Regulations, Part 71 (10 CFR 71) Packaging and Transportation of Radioactive Material. The stainless-steel structure components also provide excellent long-term performance against general corrosion and stress corrosion cracking during extended dry storage, thus enabling subsequent transportation (without repackaging of the disused CsCl capsules) to a geological repository or deep borehole for final disposal. The compact Type B packaging design also enables the use of ARG-US remote monitoring systems to enhance safety and security during extended storage, transportation, and disposal. In this paper, we will provide case studies of these two transportation packagings, illustrating the integration of safety and security by design.

References:
3. Z.H. Han, J. Li, D. Kontogeorgakos, Y.Y. Liu and J. M. Shuler, “A New Type B Packaging Design for Disused Radiological Sources,” INMM 59th Meeting, Baltimore, Maryland, USA, July 22–26,
2018.

**State**

United States

**Gender**

Male

**Primary author:** Dr LIU, YUNG (Argonne National Laboratory)

**Co-authors:** Dr SANDERS, Kenneth (Argonne National Laboratory); Mrs BENNETT IRION, Allison (Argonne National Laboratory)

**Presenter:** Dr LIU, YUNG (Argonne National Laboratory)

**Track Classification:** CC: Nuclear safety and security interfaces
Indonesia’s experience in implementing the Amendment to CPPNM for physical protection of its nuclear material and nuclear facilities

Indonesia’s experience in implementing the Amendment to CPPNM for physical protection of its nuclear material and nuclear facilities

The research and development of nuclear science and technology in Indonesia has been operating since the late 1950s, and has contributed in various sectors of life. To date, the nuclear research and development is mainly carried out by the National Nuclear Energy Agency of Indonesia (BATAN), which was established in 1958. BATAN is authorized to conduct research and development, exploration and exploitation of nuclear materials, production of raw materials for the manufacture of nuclear fuel, radioisotope production for research and development purposes, and management of radioactive waste. Various research programs and activities are focused on several important areas: energy, food, health and medicine, natural resources and environment, industry, and advanced materials for improving the welfare and competitiveness of the country. All research and development activities are carried out professionally for peaceful purposes by taking into account the principles of safety, security, and environment protection.

Indonesia has three research reactors and several supporting nuclear facilities, including nuclear fuel and radioactive waste treatment facilities, which are operated by BATAN. In addition, BATAN has also several decades of experience with operating the irradiator facilities for food preservation and medical equipments sterilization. The work at these facilities involves the use of nuclear materials and radioactive sources.

To ensure the security of radioactive material and associated facilities from various threats, BATAN has implemented security system of radioactive material according to existing standards developed by the IAEA, and maintained and strengthened the system through security systems measures.

Indonesia is a party to some international instruments of nuclear energy, especially to the Convention on the Physical Protection of Nuclear Material (CPPNM) and its Amendment, and recognizes its responsibility for establishing, implementing and maintaining a physical protection regime against theft and sabotage for all its nuclear facilities. This shows her commitment to use nuclear energy for peaceful purpose with the emphasis on safety and security. Indonesia also has a strong commitment to fully support the IAEA efforts to continually improve security system, and has cooperated with other countries for such purpose.

Indonesia recognizes the importance of promoting the physical protection (or nuclear security) objectives, and affirms its international commitment to support the strengthening of global nuclear security by ratifying and implementing the CPPNM and its Amendment. Indonesia (BATAN) has implemented physical protection of nuclear material and nuclear facilities based on such important instrument. This paper will give a description of such activities in more details.

State

Indonesia

Gender

Male
**Primary author:** HASAN, Yaziz (Bureau for Legal, Public Relations, and Cooperation, National Nuclear Energy Agency of Indonesia (BATAN))

**Co-author:** Ms PURBASARI, Ros Intan (Bureau for Legal, Public Relations, and Cooperation, National Nuclear Energy Agency of Indonesia (BATAN))

**Presenters:** Ms PURBASARI, Ros Intan (Bureau for Legal, Public Relations, and Cooperation, National Nuclear Energy Agency of Indonesia (BATAN)); HASAN, Yaziz (Bureau for Legal, Public Relations, and Cooperation, National Nuclear Energy Agency of Indonesia (BATAN))

**Track Classification:** CC: Implementation of national legislative and regulatory frameworks, and international instruments
Enhancing and sustaining regulatory frameworks for nuclear security: a work in progress

If there is one noticeable trend in nuclear security these days, it is the global effort to develop, strengthen and sustain nuclear security regulatory infrastructure. Notwithstanding the level of nuclear advancement, regulatory frameworks of any given country are primary examples illustrating the principle of continuous improvement – we can always do more, better, safer and secure. Even when a comprehensive framework is already in place, the evolving threats and the development of new technologies keep regulators busy since the frameworks need to be regularly assessed and reviewed.

A robust national legislative and regulatory framework lies at the foundation of a State’s nuclear security regime. The establishment of adequate nuclear security systems and measures against threats from malicious acts involving nuclear and other radioactive material needs a sound legal basis in order for the systems and measures to be effective, efficient, consistent and sustainable. In a fragmentary international landscape where no single international legal instrument provides a comprehensive listing of nuclear security obligations to draw from, States are in severe need of adequate expertise, resources, assistance and guidance to establish their national requirements. Nuclear security is slowly catching up with nuclear safety in that assistance in sustained regulatory development can no longer be overlooked.

The recent years have seen an expansion of activity focusing on the development of regulations for nuclear security. At the national level, States have been deploying considerable efforts to include nuclear security considerations in their nuclear legislation and regulations, while at the international level initiatives to assist with their development have started to bloom.

The paper will provide an overview of regulatory development for nuclear security throughout the world, regionally and nationally. It will analyse the current trends in regulatory development, while also giving specific examples. It will in particular provide insight into the challenges faced when developing and sustaining national nuclear security regulatory infrastructures as well as propose ideas for addressing these challenges – both at the national and at the international level – and for providing comprehensive support in this area. An overview of the initiatives undertaken to address needs in this regard will also be given. It is the thesis of this paper that enhancing and sustaining regulatory frameworks for the security of nuclear and other radioactive material is a continuous work in progress. There can be no question of setting nuclear security requirements in stone once and for all and there is no one-size-fits-all. For these reasons, identifying ways to strengthen regulatory frameworks for nuclear security concerns all States, be they small fish or big fish in the nuclear pond.

State

Poland

Gender
Primary author: Ms GIŻOWSKA, Paulina (National Atomic Energy Agency)

Presenter: Ms GIŻOWSKA, Paulina (National Atomic Energy Agency)

Track Classification: CC: Implementation of national legislative and regulatory frameworks, and international instruments
Creation and Enactment of a Computer Security Regulation for the Nuclear Industry in Kazakhstan

The Kazakhstan Regulation on Cybersecurity of the Nuclear Industry was enacted in December 2018. This regulation was the result of a multi-year cooperative agreement between the Republic of Kazakhstan’s Committee of Atomic and Energy Supervision and Control and the USA Department of Energy. This paper will provide the motivation for the creation of the regulation, overarching goals of the regulation, the processes and history of the project, and lessons learned during and after enactment.

The goal of this regulation was to create an efficient and effective computer security program at facilities which have nuclear material and/or radioactive sources. The regulation is intended to provide clear requirements for operators/licensees to follow. These requirements also provide clear expectations for the regulator to perform assessments of operators’ computer security programs. The regulation will be used to create consistency between each of operators’ computer security programs. The regulation also provides guidance and technical background where appropriate. This helps operators understand the motivations behind specific sections in the regulation. The financial and manpower burden on the operators who implement the computer security program were some of the primary design requirements of the regulation. Additionally, the financial burden on the regulator to enforce compliance was also a chief consideration. The regulation requires the regulator to assess the effectiveness of each operator’s computer security program and provide capabilities for nuclear and radiological industries in the areas of information sharing and incident response. It is also important for the regulation to assist the operator’s in the creation of long term, sustainable computer security programs.

We highlight key sections and requirements of the regulation. We will describe how this will satisfy the overarching goal of increasing the security of nuclear and radiological material. This process started with clearly understanding the goals of the regulation and the current state of computer security programs by the operators. The process required senior management representing the regulator to identify appropriate government and operator personnel to join the regulatory development team. The team required a wide array of expertise in order to ensure regulatory effectiveness. The team is included computer security experts, regulators, operators, and regulatory development experts.

Once the team was formed, the group collected and evaluated existing regulations and laws to gain an understanding of how they would interact with this new regulation. A draft regulation was then written by the team. After this, the draft regulation was shared with key stakeholders. Comments and revisions were collected and reviewed by the regulation development team. This led to more mature and complete versions of the regulation. This process was repeated until consensus was reached. We will discuss the process of getting the regulation approved and enacted. We describe how the regulation has been communicated with nuclear material and radiological sites. We will discuss lessons learned from this process. Finally, we will emphasize the importance of a robust revision process when developing national regulations.

State

Kazakhstan
Gender

Male

Primary authors: Mr ARALBAYEV, Alan (Ministry of Energy, Republic of Kazakhstan); Mr SYS- SALETIN, Andrey (National nuclear center, Republic of Kazakhstan); KURLSARTOVA, Anna (Nuclear Security Training Center, Republic of Kazakhstan); Mr BAISAGANOV, Daulet (National nuclear center, Republic of Kazakhstan); Mr BUDANBEKOV, Gabit (Committee of Atomic and Energy Supervision and Control, Republic of Kazakhstan); DE BOER, Gloria (Oak Ridge National Laboratory, USA); Mr WHITE, Greg (Lawrence Livermore National Laboratory, USA); Mr NUKUSHEV, Ibragim (Committee of Atomic and Energy Supervision and Control, Republic of Kazakhstan); Mr MOLTINERO, Matthew (International Nuclear Security, Department of Energy, USA)

Presenter: Mr ARALBAYEV, Alan (Ministry of Energy, Republic of Kazakhstan)

Track Classification: CC: National nuclear security regulations
THE CONSIDERATION OF SECURITY ASPECT IN REVIEW FOR NUCLEAR INSTALLATION OF SITING STAGE.

The security of the nuclear facilities is an important criterion for site selection and for establishing plant configuration and plant operational procedures. Plant security is ensured primarily through features that are built into the strength of the structures, configuration of the systems and layout of the buildings, and barriers and security systems which are set up to restrict access and entry into the plant. Nuclear facilities have often been designed without giving sufficient consideration to nuclear security until late in the design stage or after operational and safety features had already been determined. Nuclear security measures were added later, often resulting in the application of measures that were not integrated or fully compatible with measures relating to safety, safeguards, and operations. The facts are nuclear security in siting also influence safety aspect, therefore nuclear security must be reviewed in the site stage of nuclear installation. This paper will present consideration of the result of evaluation for site characteristics for nuclear security purposes, including review of regulation on security aspect especially for site stage when applied in Indonesia.

Keywords: security aspect, review, siting of nuclear installation

State
Indonesia

Gender
Male

Primary author: Mr HARIANTO, Rahmat Edhi (Indonesia Nuclear Energy Regulatory Agency)

Co-author: Mr ROHMAN, Budi (Indonesia Nuclear Energy Regulatory Agency)

Presenter: Mr HARIANTO, Rahmat Edhi (Indonesia Nuclear Energy Regulatory Agency)

Track Classification: PP: Nuclear security vulnerability assessments
Sustaining effective physical protection regime

Russian Federation is a party to the Convention on Physical Protection of Nuclear Material and Nuclear Facilities (including the Amendment to the Convention). In the Russian Federation, appropriate physical protection regime is established and maintained being based on fundamental principles stipulated in the Amendment.

The State Corporation ROSATOM is a competent authority in terms of international transport of nuclear material on the territory of the Russian Federation.

According to the State Corporation ROSATOM, key areas of international cooperation include:
- improvement of the quality of training in the field of physical protection;
- assistance in the development of nuclear infrastructure to newcomer countries, including the field of nuclear security and physical protection;
- provision to foreign partners of integrated proposal of nuclear facility construction including physical protection system.

The State Corporation ROSATOM has many years of experience in the capacity building and training in the field of nuclear security and physical protection. Rosatom Technical Academy extensively cooperate with the IAEA on capacity development in the field of nuclear security and assistance to newcomer countries in terms of training courses and workshops. Training programmes and training materials are based on a systematic approach to training, requirements of the Convention on the Physical Protection of Nuclear Material and its Amendment, the IAEA recommendations in the field of nuclear security and Russian extensive experience in the field. Each year, the Rosatom Technical Academy hosts several IAEA international and regional courses and seminars; in total, more than 1,100 participants from 54 countries were trained.

As a responsible vendor of nuclear technologies for newcomer countries, the State Corporation ROSATOM has experts who provide organizational and methodological support in the development of all 19 elements of nuclear infrastructure in these countries, including the field of nuclear security and physical protection. The State Corporation ROSATOM has necessary experience and methodological approach in order to provide assistance to newcomer countries with assessment of the current physical protection regime, as well as development of the required legal framework, personnel training and conducting other actions which are crucial for establishment and maintaining of physical protection regime.

The State Corporation ROSATOM has distinctive experience and resources for physical protection system development for nuclear facilities. In the Russian Federation, approach to development of physical protection system for nuclear facility is elaborated and applied; the approach is based on the IAEA recommendations in the field of nuclear security and takes into consideration Russian extensive experience in the field. Foreign partners can choose various options of physical protection system as a feature to the integrated proposal of nuclear power plant or centers of nuclear science and technology construction. In the process of physical protection system development, national requirements and the IAEA recommendations are taken into consideration. Russian proposal for physical protection system development consists of two parts: technical (engineering and technical physical protection equipment complex) and documental part (documents required for physical protection system functioning in the facility).

The State Corporation ROSATOM has unique experience in development of physical protection system for small modular reactors.
State

Russian Federation

Gender

Primary authors: Mr DENISOV, Konstantin (State Atomic Energy Corporation "Rosatom"); Mr BAYCHURIN, Ruslan (State Atomic Energy Corporation "Rosatom"); Mrs AFANASYEVA, Taistyia (State Atomic Energy Corporation "Rosatom")

Presenter: Mr DENISOV, Konstantin (State Atomic Energy Corporation "Rosatom")

Track Classification: PP: Security by design, including in newcomer countries
The Current Status of Detection Infrastructure Development in Indonesia

As an archipelagic country, Indonesia has more than 150 ship ports. Ten of the international ports are providing online services. However only six of them are equipped with radiation portal monitors (RPMs). The procurement of these RPMs were done both through international cooperation and independent purchasing. Indonesia has many land borders in three islands, namely Kalimantan (Borneo), Papua, and Timor. At this time, these land borders are not equipped with RPM. It also happened that none of the almost 30 international airports in the country are not equipped with RPM. In 2018, Indonesia cooperates with the IAEA as written in Integrated Nuclear Security Support Plan (INSSP), for the application of nuclear security measures at a major public event, the Asian Games XVIII in Jakarta and Pelembang City. Furthermore, industrialization in Indonesia is also rising significantly in recent years. In other side, while Indonesia provide a gift basket in The Hague 2014 Nuclear Security Summit in the form of Nuclear Security Legislation Implementation Kit document, in fact, Indonesia is still in groundwork for the establishment of national nuclear security law.

All of the above matters can be considered as both opportunities and challenges, which underlined the importance of nuclear security and strengthening efforts of national commitment to it. While legislation is in preparation, technological issues should also be faced. For this, Indonesia is not only maintaining international cooperation but also is in its progress on developing RPM technology domestically. With this project, it is expected that the number of RPM could match the national needs and that the operation and maintenance could be sustained. This paper will describe the current industrial development in general, situation of the RPM operation and the technology development process and achievement.

The multi-year national project for RPM technology development engaged many national institution as a part of national nuclear security regime entity, such as research institutes, university, state own company and competent/regulatory authorities. The roles of related institutions have been defined and the scheme of cooperation have been established, completed with flexible government funding schedule. Architecture design of the RPM, comprised of detection equipment, CCTV, CAS, and power supply and I&C, have been implemented. Field testing have been carried out with instalment and operation of the RPM prototype in the main gate of National Nuclear Energy Agency (BATAN) facility in Serpong Town, Banten Province, near Jakarta. Some operational feedbacks have been collected. The next step is regarding standardization and certification for this product. Early preparation is in progress. This is including identification of all necessary standards and testing facilities and equipment, and gap analysis with the current situation. Completed program for 2020-2024 period is being formulated. Indeed, many constraints and challenges have to be managed. In overall, with this national project Indonesia is learning in research and development on RPM technology, while also demonstrate its commitment to sustaining nuclear security regime.

State

Indonesia

Gender

Male
Primary authors: Mr ALAMSYAH, Reno (BAPETEN (Nuclear Energy Regulatory Agency)); Mr PRISTIANTO, Agus Yudhi (BAPETEN); Mr KHAIRUL, Khairul (BATAN); Mr KURNIANTO, Kristedjo (BATAN)

Presenter: Mr ALAMSYAH, Reno (BAPETEN (Nuclear Energy Regulatory Agency))

Track Classification: MORC: Detection technology development and performance testing
Nuclear security culture - the what, the why and the how!

As wholly owned subsidiary of the UK’s Nuclear Decommissioning Authority (NDA), International Nuclear Services (INS) has extensive and proven experience in the transportation of nuclear materials both in the UK and around the world. INS and its subsidiary, Pacific Nuclear Transport Limited (PNTL), are recognised as the world’s most experienced nuclear shipping company having delivered over 180 shipments of new & spent fuel, active waste and specialist nuclear material over their 40 year history. Last year, INS completed an unprecedented number of Category I transports of nuclear materials on-board its purpose built nuclear transport vessels, and in doing so, continues to support the UK and other States in their efforts to discharge their nuclear security commitments.

In addition to these important shipments INS also provides security and resilience consultancy services around the world to a number of customers and is a consortium member of the UK’s Global Nuclear Security Programme (GNSP) where alongside Kings College London (KCL) and Amport Risk Ltd, it helps deliver a number of security workshops and educational activities to help further improve the understanding and exchange of learning around nuclear security topics globally. In doing so, INS uses the capabilities it and PNTL has developed over its 40 year history to share its practices and approaches to various nuclear security disciplines.

A key element of INS’s security arrangements is the establishment and delivery of a targeted ‘Security Culture & Awareness Programme’. As we all know, having a strong and sustainable nuclear security culture is essential to the success of an organisation’s security arrangements – people, their behaviours, values and beliefs can and will have an impact on the performance of your security system and its effectiveness. This paper will initially look at the organisational benefits a strong security culture will bring, and the risks you may face if you have a poor or inadequate security culture. It will also discuss how security culture overlaps with other business sub-cultures, such as nuclear safety culture, and the benefits and challenges of working collectively to maximise functional benefits across the business.

The second part of this paper will describe how INS constructs its ‘Security Culture & Awareness Programme’, taking account of both its assessment of organisational risk, trends and intelligence. It will discuss the methods in which we deliver these activities to ensure organisational learning is optimised, giving examples of successful and unsuccessful activities. Finally, it will also outline the ways in which we gain assurance of the strength of our security culture through various means including questionnaires, tests and interviews. In doing so, it is hoped this paper will help other States and organisations understand how INS approaches security culture and encourage continued shared learning.

State
United Kingdom

Gender
Male
Primary authors: WHITTARD, Ben (International Nuclear Services Ltd); BURGUL, Rakesh (International Nuclear Services)

Presenter: WHITTARD, Ben (International Nuclear Services Ltd)

Track Classification: CC: Nuclear security culture in practice with a focus on sustainability
Steganographic and covert communication is increasingly used for hiding attacks. The analysis of such criminal use of information hiding is also subject of the CUIng initiative \[1\] which cooperates with the Europol European Cybercrime Centre. Often information hiding is used by attackers in advanced persistent threats in order to operate without being noticed. Attackers might use it to hide data exfiltration or control channels for persistent malware.

Within the scope of industrial automation systems in general and nuclear instrumentation and control systems (I&C) in particular, information hiding is a new application field. This paper’s objective is the analysis of existing attacks utilizing information hiding in the information technology (IT) domain, such as the Turla Backdoor \[2\] which could exfiltrate files, execute commands or download and execute files via an Exchange mail server, and their projection to the operational technology (OT, I&C) domain. In conjunction with that, attacker models are created, which might be used to extend the cyber design basis threat (cyber DBT). As a foundation the paper will summarize the general setup of I&C systems based on IEC 62443 \[3\] and zone concepts from IAEA Nuclear Security Series draft NST047 \[4\]. Based on this generalized architecture model, potential cover channels and the suitability of I&C specific communication for steganography are identified and analyzed. Such cover channels are formed by the usual communication within the I&C system including, but not limited to, Modbus/TCP, OPC UA, Syslog, etc. Using the generalized architecture model and the communication flows, the attack potential using information hiding is exemplary assessed. Subsequently, recommendations for a strategic and operational preparation for operators towards the prevention and detection of information hiding attacks are derived.

Information hiding can be used for different purposes. In the media it is widely used in invisible watermarking, e.g. for digital rights management. In communications, information hiding can be used to hide communication channels within normal network traffic. The objective of such hidden channels could be threefold: data exfiltration (unidirectional communication), data injection (unidirectional communication), command and control (bidirectional communication). The communication channel can be formed as a timing or a storage channel. In timing channels the existing communication is modified, e.g. by delaying network frames. In a storage channel the network frames are modified in order to embed the data. In the latter case it is crucial that the original purpose of the message is not influenced, otherwise the covert channel could be easily detected. A third option would be the introduction of additional network frames. However, such frames need to seem authentic and should not influence the processes at all.

For the threat analysis we use IEC 62443 \[3\] for I&C systems in combination with the zone concepts of NST047 \[4\]. With the required services such as Syslog for a secure operation of the equipment or the communication of process data via OPC UA, e.g. to a process and plant historian, several security zone border crossing network communication exist. Such communication is a suitable cover channel for information hiding. In particular, we consider scenarios for data exfiltration, also considering unidirectional communication, e.g. via data diodes, data injection, e.g. for triggering specific actions as well as a bidirectional command and control communication. For each scenario the communication across the different security zones is analyzed in order to estimate potential communication flows and the necessary effort for a successful attack. The analysis of the effort for the attack vectors considers potential infection vectors ranging from malware infection to directed attacks via the supply chain.

The general possibility of information hiding is demonstrated based on a small setup recreating the turbine governing system including the communication of this subsystem via OPC UA. Based on this setup the peculiarities of the I&C network communication are discussed and compared to standard IT systems. The paper will discuss the placement of network probes in order to prepare...
a detection of hidden communication channels. The main challenge, besides the mere detection of covert communication channels, is the concept of discovering such additional functionality during an assessment prior to the deployment of a component.

References:
Contribution of the Vienna Center for Disarmament and Non-Proliferation to Nuclear Security: Building Consensus and Expertise through Outreach and Training

The role of the International Atomic Energy Agency (IAEA) regarding nuclear security evolved after the terrorist attacks of September 11, 2001, and the IAEA is currently held to be the global platform for nuclear security efforts, with a central role in facilitating international cooperation in the field. However this evolution has not been effortless, and universal acceptance by Member States of nuclear security as a vital component of the IAEA’s role in global nuclear governance, remains elusive. Among a number of reasons for that there are varying degrees of knowledge and capacity for nuclear security implementation between Member States and, whilst the IAEA has been playing and continues to play a central role in meeting nuclear security capacity building demands, the needs of Member States far outweighing the resources available to the IAEA. Member States maintain seemingly intractable positions about the funding of the IAEA’s nuclear security activities and the role of nuclear security vis-a-vis peaceful uses of nuclear energy and nuclear applications. Building consensus on nuclear security in the IAEA requires a concerted effort to change this dynamic between Member States. The Vienna Center for Disarmament and Non-Proliferation (VCDNP) is contributing to consensus building by promoting a better dialogue between Member States on nuclear security practices and their impact on the peaceful uses of nuclear energy and nuclear applications. In order to be constructive, this dialogue has to be factually based and result in a better understanding of the challenges faced and efforts made by Member States and the IAEA to improve nuclear security when applying nuclear technology for peaceful uses.

In April 2018 the VCDNP embarked on a series of panel discussions with the aim to create opportunities for dialogue between technical experts and diplomats on the benefits of the peaceful uses of nuclear technology, the challenges related to the safe and secure management of nuclear and other radioactive materials and related facilities, and the support provided by the IAEA to its Member States. These panel discussions have been well attended by diplomats and other nuclear professionals from a broad range of countries, who have commended the VCDNP on increasing their knowledge and understanding of the benefits of peaceful uses, the role and importance of nuclear security and the support provided by the IAEA. The VCDNP is also producing fact sheets related to the panel discussions, which serve as an additional source of information for diplomats and policy makers.

The VCDNP also developed a nuclear security course to support capacity development in Member States, which complements the IAEA activities enshrined in its Nuclear Security Plan 2018-2021. The first VCDNP Nuclear Security Professional Development Course took place in February 2019 and was targeted, inter alia, at the nuclear energy policy makers, regulatory staff and diplomats of newcomer states. The purpose of this course is to enhance participants’ understanding of key nuclear security-related issues, including the history of the nuclear security regime, legal framework and other international instruments, the role of the IAEA and other organisations, opportunities and challenges related to nuclear security, and the policies and politics of nuclear security. The course programme included presentations and practical exercises on nuclear security issues delivered by IAEA and other international experts.

The 21 participants from nuclear newcomer states confirmed that the course contributed significantly to their knowledge and to their professional development in the field of nuclear security.
This course will be expanded in future to include diplomats from other Member States, to meet the
demand in this regard and to support the VCDNP’s goals of promoting a better dialogue between
Member States on nuclear security and to contribute to achieving consensus on nuclear security
in the IAEA.

State
Austria

Gender
Not Specified

Primary authors:  Ms KIRSTEN, Ingrid (Vienna Center for Disarmament and Non-Proliferation); Mr
LAZAREV, Artem (Vienna Center for Disarmament and Non-Proliferation)

Presenters:  Ms KIRSTEN, Ingrid (Vienna Center for Disarmament and Non-Proliferation); Mr
LAZAREV, Artem (Vienna Center for Disarmament and Non-Proliferation)

Track Classification:  CC: Capacity building (e.g. human resource development and sustain-
ability, nuclear security education and job-specific performance training including for new-
comer countries)
You Only Get One Chance to Make a First Impression: Keys to a Successful Amended CPPNM Review Conference

The review conference for the amended Convention on the Physical Protection of Nuclear Material (CPPNM) that is set to take place in 2021 will be the first of its kind, following the Amendment’s entry into force in 2016. This presents an important opportunity to lay the groundwork for a process that will both help facilitate full and effective implementation of the treaty and provide a forum for the parties to discuss needs for eventual evolution of the treaty regime in light of changing circumstances. In other words, as laid out in Article 16, review conferences under the amended CPPNM have a dual function, to look both at the implementation of the treaty as well as its adequacy. The reference in the Article 16 to “adequacy” means that the very suitability of the treaty to realize the aims that led to its adoption is part of the review discussion, in addition to operation of the treaty. It is an added element, requiring parties to go beyond article-by-article analysis, that leads one to believe that the process under the amended CPPNM is designed to involve broader consideration and debate of nuclear security requirements and how the treaty contributes to nuclear security governance. However, the review conference provision of the treaty unfortunately provides no guidance on the procedure or substance of the review conference. This paper will elaborate five keys, both substantive and procedural, to a successful 2021 review conference. First, the review conference agenda should not only give parties the opportunity to discuss implementation practice, challenges and lessons learned, but also should include a discussion of the treaty’s ability to deal with emerging threat and challenges. Second, parties should agree on the role of the Nuclear Security Series Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (NSS No. 13, INFCIRC/225/Rev.5) as implementation guidance for the amended CPPNM, and call for this non-binding instrument to be updated regularly. Parties could agree, unanimously or by consensus depending on the rules of procedure adopted for the review conference, that the provisions of INFCIRC/225/Rev.5 are the appropriate measures necessary for establishing, implementing and maintaining an appropriate physical protection regime applicable to nuclear material and nuclear facilities under a state party’s jurisdiction (Article 2A). Third, parties should commit to undergoing International Physical Protection Advisory Service missions (including follow-up missions) in order to assess the state of national nuclear security regimes, and should commit to acting in accordance with the missions’ recommendations. Fourth, states should make a commitment to share information on laws and regulations giving effect to the treaty, as required by Article 14, and provide updates as necessary. Article 14 is an obligation of notification, providing no guidance on the format of information to be provided and leaving the amount of detail to be provided up to the discretion of the party concerned. Parties could make use of the template proposed by the Netherlands for sharing nuclear security-related information, as a way to harmonise the type of information shared and to assist parties with limited reporting capacity. The more information provided, the better it serves to build trust and confidence in compliance with the treaty, and the information provided by states parties could form the basis for discussing issues related to implementation and adequacy during review conferences. Finally, parties should agree to the convening of further review conferences in the interest of ensuring the continued viability of the treaty framework. With these five keys, the review conference for the amended CPPNM can become an effective instrument for strengthening the international legal framework for nuclear security.
State

Netherlands

Gender

**Primary author:** Dr HERBACH, Jonathan (European Leadership Network)

**Presenter:** Dr HERBACH, Jonathan (European Leadership Network)

**Track Classification:** PP: The Amended Convention on the Physical Protection of Nuclear Material review conference in 2021
Vulnerability assessment of Nuclear Security Systems in Kenya

In Kenya, Nuclear and Radioactive material are utilized in medicine, agriculture and Industry. Aside from these sectors there exists, 2 irradiators and a Central Waste Processing Facility (CWPF) and many mobile sources that could be targeted by adversaries. Like many other countries, Kenya has had its share of nuclear security incidents from both internal and external adversaries. For example, in 2016, a Multi-agency undercover operation was conducted by Directorate of Criminal Investigation- Bomb technicians, National Intelligence Service and Kenya Wildlife Services in Lang’ata. It was alleged that there was an Improvised Explosive Device hidden in one of the houses. This operation led to recovering of a Cesium 137 source. A serving and a retired Kenya Defense Forces’ officers with a civilian were arrested in connection to the source. The matter is still in court and investigations in connection to the source origin is still on going. The source was being sold at a price of USD 8,000,000. It is possible that the source could be from the armed forces leading to the question on accountancy and control of nuclear and radioactive material. There have been many other incidents involving theft and loss of mobile sources used in well logging, moisture density gauges as well as in industrial radiography. In most of these incidents, information from the public has helped the regulatory body in recovering of the sources. It is evident that members of the public can be a good source of information on such incidents. It is therefore important as the regulatory body to create a platform where the public can reach you. It also portrayed that there is an active threat on radioactive material which could be targeted by adversaries.

Kenya has faced many terrorist attacks namely; the bombing of the US Embassy by the Al Qaeda and the West gate mall attack by the Al Shabaab among other attacks coupled with several criminal groups who could target radioactive material to perpetrate their violent attacks. Radioactive material such as Cs-137 in the hands of adversaries could be a prime component in making a Radiation Dispersal Device because of its potential to be dispersed. Given the many threats that are present in the country, the Radiation Protection Board has conducted a vulnerability assessments from the Nuclear Security incidences that have occurred as well as the mitigation and response strategies in place to prevent against acquisition of Nuclear and Radioactive material by non-state actors.

State

Kenya

Gender

Female

Primary authors:  Ms MURIITHI, Mercy (Radiation Protection Board); Mr MUNDIA, Isaac (Radiation Protection Board)

Presenters:  Ms MURIITHI, Mercy (Radiation Protection Board); Mr MUNDIA, Isaac (Radiation Protection Board)
Track Classification: PP: Nuclear security vulnerability assessments
Systematic Approach to Safety and Security; Challenges and Opportunities

National nuclear programs consist of different nuclear and radiological activities with advanced technologies operating in a complex regulatory environment. It shall consider the development of proper organizational culture for nuclear safety and nuclear security that involves the key organizations and individuals in a number of diverse disciplines; who must work together in harmony to be effective. Within the nuclear industry the work performance is directly related to human, organizational and cultural factors that when untoward events happen they cannot be scaled down to the failure of any single element or component. Rather, events emerge from the dynamic interactions between number of factors as knowledge, decisions, thoughts, emotions, actions, physical technologies, equipment, management systems, knowledge management, organizational structure, governance, and human and financial resources. Harmonization the development of nuclear safety and security culture and handling the interfaces between them is great global concern. The paper introduces the importance of generation analysis for the nuclear leaders and gives recommendation on the motivation tactics based on the generation map of Egypt. Apply the systemic approach to safety and security within the nuclear interested parties address these risks by examining how the complex interactions between human, technical, and organizational factors produce safety and security on a day-to-day basis. But it has to consider the nature of the organization if regulator, owner, vendor, or others, and the main features of the national culture. The work show the challenges and opportunities of using the systematic approach for safety and security taking into consideration the generation map and the specific characteristics and behaviors of each generation.

State
   Egypt

Gender
   Female

Primary author: Dr GOMAA, Rania (Supervisor of Management System General Administration)

Presenter: Dr GOMAA, Rania (Supervisor of Management System General Administration)

Track Classification: CC: Nuclear safety and security interfaces
Cambodia’s Participation in Coordinated Research Project (CRP)

In this presentation, we will look at the results of Cambodia’s participation in the Coordinated Research Project (CRP) and how the mobile application “Tool for Radiation Alarm and Commodity Evaluation (TRACE)” will help users, especially Front Line Officers (FLOs), to reduce the hurdle of Initial Alarm Assessments and random inspections and focus on the most suspicious containers.

Under the Memorandum of Understanding (MoU) between the United States and Cambodia, represented by the United States Department of Energy (USDoE) and Secretariat of National Counter Terrorism Committee (SNCTC), it was decided that 6 Radiation Portal Monitors (RPMs) be installed in Sihanoukville Autonomous Port at the container gate in 2011 and 4 more at the entrance and exit of railyard in 2018. Since the early stage, Customs officers have been playing the main role in operating the system; and Secondary Inspections (SI) on containers have been made to prevent any potential nuclear risks from coming in and going out of the country. To decide for SI, officers are trained to look at different criteria such as Alarm Profiles, Sigma Values and Commodity Information, to name a few. However, the high volume of the flow of containers in and out of the port leads to high number of secondary inspections, which requires a lot of hard work. Moreover, Customs officers have to be rotated from one checkpoint to another after a few years of service. This poses even more challenges to the operation because assessing the alarms also requires some knowledge of the Alarm Assessment itself. Thus, it becomes quite challenging for new officers who come after official trainings. Faced with the problem, we need a solution to this challenge to both improve the efficiency of the assessment and reduce the number of random SIs and focus on the most interesting containers.

The International Atomic Energy Agency (IAEA) initiated Coordinated Research Project (CRP) with the period covered from 2015 to 2019 to collect and analyze data in order to improve alarm assessments and to develop TRACE that can help users assess the alarms faster and more reliably at the initial stage. As one of the member states having participated since 2015, and in contribution to the CRP, Cambodia submitted more than 100 datasets of 8-point Secondary Inspections using Radiation Isotope Identification Devices (RIIDs) and various testings in 2017, datasets of Alarm Records in 2018 and will submit more datasets in 2019 and also conduct “TRACE Beta Testing” to conclude the project.

As a result, TRACE proves to be a very useful and reliable reference tool for FLOs in daily duties. It provides faster analysis and more confidence to the officers and also requires little time and efforts for training new comers, thanks to its intuitive user interface and features.

State

Cambodia

Gender

Male

Primary author:  Mr SENG, Sovath (Customs officer of the General Department of Customs and Excise of Cambodia (GDCE))
Co-author: Mr UNG, Eang (Secretary of State of Ministry of Mine and Energy and Vice President of Secretariat of National Counter-Terrorism Committee.)

Presenters: Mr SENG, Sovath (Customs officer of the General Department of Customs and Excise of Cambodia (GDCE)); Mr UNG, Eang (Secretary of State of Ministry of Mine and Energy and Vice President of Secretariat of National Counter-Terrorism Committee.)

Track Classification: CC: Innovative technologies to reduce nuclear security risks and improve cost effectiveness, where feasible
Nuclear and Other Radioactive Material Transports in the Maritime Environment: ‘Evidence over Assertion’ - Assuring the International Community

Question - how does the world’s leading Special Nuclear Material and Radioactive Material Shipper assure its own competent authority and the international community that it can safely and securely transport every conceivable cargo on the Radioactive Material spectrum? Answer - through employment of rigorous and robust internal and external assurance programmes.

International Nuclear Service (INS), part of the United Kingdom’s Nuclear Decommissioning Authority (NDA), has been doing just that for well over 40 years by road, rail and sea. Today the NDA’s estate has a wealth of transport expertise including consignor/consignee knowledge, transport flask design and licensing, emergency response and radiation protection, safety, security and transport and lifting operations. In doing so, it has transported some of most sensitive nuclear materials, including plutonium and high enriched uranium, both domestically and internationally. As one can imagine, transports of this nature are essential and act as a critical enabler to the nuclear sector and its fuel cycle.

Integral key stakeholders and indeed the target audience during this process include the Coastal and Shipping States community, international governments and competent authorities, as well as the wider international community, for example non-governmental organisations (NGOs) and not least the general public through utilisation of, amongst other media, corporate communications. Not forgetting that clear and concise underpinning legislative and regulatory frameworks are pivotal in directing and informing a proportionate yet effective safety and security provision.

Radioactive Material is a ‘broad church’ governed by different areas of legislation. Regarding nuclear material, the CPPNM entered into force on 8 February 1987 which, inter alia, established physical protection measures that had to be applied to nuclear material in international transport. Thereafter in 2005 the Parties to the Convention achieved consensus for an Amendment, which entered into force on 8 May 2016. The Convention and the Amendment form the single legally binding international instruments in the area of physical protection of nuclear material.

The key point therein pertains to what were previously considered obligations for physical protection under the CPPNM, however, post entering into force are now legally binding for States Parties in order to protect nuclear material during transport but NM is only one part of the conundrum.

For what is termed Other Radioactive Material (ORM), from a shipping perspective, governance is achieved via employment of a number of documents, including the IAEA Code of Conduct on the Safety and Security of Radioactive Sources (the ‘Code’) and the UNECE Orange book (UN Recommendations on the Transport of Dangerous Goods Model Regulations). Furthermore, the IAEA SSR-6 Transport Regulations (outlining guidance on the safe transport of radioactive material) aids formation of the basis of international modal regulations established by other United Nations bodies, such as the International Maritime Organisation’s, namely, the International Maritime Dangerous Goods (IMDG) code which is holistically fused to provide optimal safety and security standards in the transportation of everything from vitrified high level waste reprocessing returns to spent fuel and radioactive sources.

At the high end of the continuum, and in order to deliver safe and secure Category I nuclear material maritime transports International Nuclear Services (INS), in conjunction with its strategic partner the Civil Nuclear Constabulary (CNC), Her Majesty’s Royal Navy, and with the agreement and approval of the United Kingdom’s Office for Nuclear Regulation (ONR), has developed a rigorous and robust quality assurance and operational capability check to ensure both internal and
external expectations are met in terms of understanding, timeliness, completeness, and value. This INS bespoke Maritime Integration Training and Demonstration (MIT/MID) programme has been designed specifically to counter the threat posed from maritime and nuclear sector threat actors and vectors and has been successfully employed in advance of numerous live international and national security operations.

In tandem and symbiotic to this, contingency in the form of Emergency Preparedness and Resilience (EP&R) functionality is similarly exercised and scrutinised with a view to delivering a testing and pressurised environment not only at the operational and tactical levels but on the ‘government to government’ communications level via, principally, the Coastal and Shipping States forum and through international exercises conducted at the IAEA’s Incident emergency Centre in Vienna.

In summary, this paper will elucidate further in support of the above assertions providing detailed evidence on how credible assurance is designed, delivered and audited with a view to overcoming the challenges presented by an ever more dynamic and evolving threat environment and in doing so inform the reader on how the global leader in this area engenders confidence in its professional capabilities.

**State**

United Kingdom

**Gender**

Male

**Primary author:**  Mr OFFICER, Robert (Industry)

**Presenter:**  Mr OFFICER, Robert (Industry)

**Track Classification:**  PP: Transport of nuclear and other radioactive material: practices, challenges and regulatory issues
Organizational Governance Template for Nuclear Security

Abstract
As emerging technologies pose new attack vectors to critical infrastructure, including nuclear facilities, the nuclear sector must navigate a business environment that is growing heavily tech-dependent while maintaining security of highly sensitive information and materials. In particular, operators must cultivate a sense of trust with key stakeholders – shareholders, regulators, the public – by demonstrating transparency and building a reputation as nuclear security champions.

Nuclear facilities are required to meet an estimated range of adversary characteristics that are established by each State in accordance with the State’s Design Basis Threat (DBT). While a proven degree of strong protection measures are required to license a facility, it is another matter to cultivate an approach to good governance that also demonstrates due diligence and management accountability. Good governance includes a broader, enterprise-wide assessment of security risk that balances economic tradeoffs with increasing security costs and profitability. Facilities must support a workplace culture (beliefs, values, and attitudes) that impresses upon stakeholders the credibility of security threats and the role of all involved in the enterprise to remain vigilant.

Stimson’s Organizational Governance Template for Nuclear Security is a resource that offers a series of questions for executive managers and senior leadership in nuclear facilities to describe their process of building and sustaining a proactive security governance approach and a robust security culture that is responsive to emerging challenges. Answering these questions is an opportunity for an organization to review its organizational decision-making process on security-related matters and how it ultimately impacts the beliefs and attitudes of the operational-level workforce tasked as responsible stewards of nuclear materials and technologies. The governance template process not only captures the core nuclear security culture, but more importantly, the governance and decision-making process of an organization. Stimson is currently working with one of the world’s largest nuclear operators to prototype and customize the governance template to the needs and requirements of their organization in a way that protects proprietary information, enhances transparency, and integrates the outcomes and recommendations into existing workflows. The governance template helps improve security processes and policies by cultivating a model of good organizational governance. This model also informs and shapes nuclear security culture into a narrative that is understood and meaningful to core stakeholders – shareholders, regulators, and the public.

This paper will present the findings from Stimson’s prototype and consultative process with a nuclear operator in the fall of 2019. By the end of the consultation, we will have produced a snapshot of the operator’s nuclear security governance framework and associated culture and developed recommendations with the operator for further implementation of its customized nuclear security governance template. The long-term goal is for industry to utilize the governance template to evaluate and enhance nuclear security governance at their facilities and socialize the template’s benefits with other industry stakeholders. Thus, the template could serve as an internal risk assessment/gap analysis tool for the nuclear sector to determine whether senior leadership has a consistent understanding of, and commitment to security by way of policy and practice. Furthermore, continued industry input will allow the governance template to be a flexible tool that can be adapted and modified for the broader nuclear/radiological sectors in different regions of the world.

State
United States
Gender

Male

Primary authors: Mr KIM, David (The Henry L. Stimson Center); Ms UMAYAM, Lovely (The Henry L. Stimson Center)

Presenter: Mr KIM, David (The Henry L. Stimson Center)

Track Classification: CC: Contribution of industry to nuclear security
A prototype of a new virtualized secure embedded product for Operational and Safety Related I&C Functions

Virtualization technologies were developed first by the information technology (IT) industry. Now they have started being deployed in the process industry. Virtualization is a set of technologies that can be applied to a wide variety of applications and fields. Hardware and/or software can be virtualized: Hardware virtualization can be deployed in the process automation, where process engineering departments supervise the process application software. Current technologies, specifically virtualization alongside fault tolerance and more reliable hardware and software components, are able of making plants operate smarter, faster, safer, and also facilitating the overall management system. Before, virtualization was an unknown concept for industry, nowadays some companies have chosen to deploy virtualization also for its benefits in terms of cost savings. As virtualization technologies keep growing, new implementations and improvements are rising. Some of the emerging virtualization technologies can be challenging to deploy for project managers and integrators. Currently, numerous organizations are implementing virtualization technologies on the server’s side; in order to lower their power consumption, optimize facilities’ space and surface requirements which are related to servers’ implementations. In terms of conserving Confidentiality, Integrity and Availability (CIA) requirements, virtualization technologies are able of providing high availability for critical applications. Virtualization capabilities go beyond simplifying IT processes, it permits IT organizations to react rapidly to the varying business requests. The growing complexity, variety and diversity of products and also long innovation’s phases present some of the important challenges surrounding products’ developments within factories and plants. Virtualization’s product development is a possible solution to deal with these challenges. By adopting diverse virtualization technologies (VT) products can be developed faster, cost effectively and with a higher quality. On the other hand, virtualization technologies necessitate novel skills within organizations and also operations. In some cases, multiple applications with different levels of criticality are implemented in the same platform even though each application requires a different level of security.

In this paper, an architecture of a new secure platform based on virtualization will be presented. In this prototype, security is applied both in the software layer and the hardware layer as well. This architecture can potentially be applicable for Industrial Automation and Control Systems (IACS) of Industry 4.0 but also for Safety Instrumentation & Control (I&C) and Operational I&C in Nuclear Power Plants. In this paper, we will list most common security, scalability and legacy issues surrounding traditional I&C systems and explain how the proposed architecture can solve some of the security concerns. With regard to functional safety and nuclear safety a graded approach is necessary for both, safety and security. In this paper the focus will be on improved security while the impact on safety according to IEC 62589 is considered as boundary conditions.
Female

**Primary author:**  TELLABI, Asmaa (Framatome GmbH/University of Siegen )

**Co-authors:**  Dr WAEDT, Karl (Framatome GmbH); LOU, XinXin (Framatome GmbH); SABRI, Abdelbast (FAU)

**Presenter:**  TELLABI, Asmaa (Framatome GmbH/University of Siegen )

**Track Classification:**  CC: Information and computer security considerations for nuclear security
German-Ukrainian Cooperation in Nuclear Security

We report about milestones, past challenges, and the way ahead for a successfully ongoing German-Ukrainian nuclear security cooperation programme, which was launched in 2015 under the auspices of the Global Partnership against the Spread of Weapons and Materials of Mass Destruction. Following a thorough needs assessment, two sites were selected for implementation: 1) Rivne Nuclear Power Plant (RNPP), located in Varash about 360 km northwest of Kiev, and 2) South Ukraine Nuclear Power Plant (SUNPP), located near the city of Yuzhnoukrainsk approx. 350 kilometers south of Kiev.

The project in Rivne NPP aims at advancing the physical protection of power unit 3 and involves the retrofitting of the inner security perimeter by modernizing access control, intruder detection, video surveillance, and physical barriers, as well as by integrating the upgraded systems into the plant’s central alarm station.

The project in South Ukraine NPP focuses on modernizing and fortifying the site’s outer perimeter including the fence system, access points for railway and cars, and guard stations.

State

Germany

Gender

Primary authors: Dr KAMPRAD, Alexander (Federal Foreign Office of the Federal Republic of Germany); Mr RDUCH, Alexander (Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH); Mr MAKARENKO, Oleg (SE "NNEG "Energoatom")

Presenters: Dr KAMPRAD, Alexander (Federal Foreign Office of the Federal Republic of Germany); Mr RDUCH, Alexander (Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH); Mr MAKARENKO, Oleg (SE "NNEG "Energoatom")

Track Classification: PP: Nuclear security of nuclear fuel cycle facilities: emerging technologies and associated challenges and complex threats
Overview of the World Nuclear Transport Institute’s (WNTI) Transport Security Working Group (TSWG)

The World Nuclear Transport Institute (WNTI) was founded in 1998 by British Nuclear Fuels plc (BNFL), now International Nuclear Services (INS) of the United Kingdom, COGEMA now Orano of France, and the Federation of Electric Power Companies (FEPC) of Japan to represent the collective interests of the radioactive materials transport sector, and those who rely on safe, effective and reliable transport. 20 years after its establishment, WNTI now represents the views and interests of over 45 members from across the world. WNTI is based in London but has representatives across the globe including Australasia, China, Japan, North America and Southern Africa. Its members range from consignors, consignees and carriers, to engineering specialists, insurers and legal entities. Its membership is diverse, and it is dedicated to effectively representing its membership and acting upon their needs and requirements.

In doing so, WNTI hosts a number of specific member working groups which come together twice a year at its Semi Annual Members Meeting (SAMM). These working groups represent the key areas in which the members work together to ensure WNTI’s mission is achieved, discussing key risks, issues and sharing good practice. These working groups include; the SSR-6 industry working group; the Uranium Concentrates Working Group; the Back End Transport Working Group; the HEXT Working Group; and the Transport Security Working Group. Each working group is chaired by WNTI’s members whom are supported by a WNTI Specialist Advisor with engagement from across the entire membership.

This paper will specifically provide an overview of the activities and priorities of the WNTI Transport Security Working Group in 2019/20 and how it has contributed to the sector more widely, including at the International Atomic Energy Agency (IAEA), International Maritime Organisation (IMO) and at the United Nations (UN). In doing so, it will describe its organisation and management, its work completed to date, including an overview of the relevant good practice it has created in coordination with the World Institute for Nuclear Security (WINS), and its work plan, which centres around three central pillars; learning from experience (LfE), industry voice and competency. It will also discuss the benefits of WNTI’s observer status at the IAEA and the work it has done with the IAEA and other international organisations to represent its members views and opinions. To conclude, it will discuss the Transport Security Working Group’s future work programme and the areas of interest that its members have raised.

State

United Kingdom

Gender

Male

Primary author:  WHITTARD, Ben (International Nuclear Services Ltd)

Presenter:  WHITTARD, Ben (International Nuclear Services Ltd)
Track Classification: PP: Transport of nuclear and other radioactive material: practices, challenges and regulatory issues
The U.S. Cesium Irradiator Replacement Project (CIRP): Successes to date and efforts to engage U.S. sites

The Cesium Irradiator Replacement Project (CIRP) was established by the U. S. Department of Energy National Nuclear Security Administration’s Office of Radiological Security (ORS) as part of its three-pillar approach to radiological material risk reduction. The first two pillars focus on enhancing security of existing radioactive sources and on removing disused radioactive sources. The third pillar, encompassing CIRP, is focused on reducing radiological materials by encouraging the transition to non-radioisotopic alternative devices, where possible, to achieve permanent risk reduction. However, unlike several countries in which using alternative technologies is mandatory because the use of cesium chloride is banned or significantly curtailed, such as in Norway and France, CIRP is voluntary. As a result, meeting risk reduction goals requires creative approaches to encourage sites to switch from cesium and cobalt to an alternative technology. This has included consistent outreach and education in various forums to organizations operating radioisotopic devices to stimulate interest in considering alternative technologies. The voluntary nature of the program has also required the creation of an effective incentive structure, the need to address site concerns, such as the appropriateness and reliability of the alternative technology, establishment of a disposition pathway for the disused sources, and a method for gathering operational data from sites that switch from cesium and cobalt to an alternative technology. This data is used to help recruit additional volunteer sites. In the roughly 4 ½ years since CIRP began, the program has achieved permanent risk reduction by eliminating and replacing 83 cesium and cobalt devices with alternative technologies. This has included commitments by two large U.S. organizations to replace the vast majority of their cesium and cobalt devices with alternative technologies; the University of California system and New York City.

Achieving risk reduction goals in the U. S. by voluntarily eliminating the use of cesium chloride became more urgent with the passage of the 2019 U.S. National Defense Authorization Act (NDAA), which was signed into law on August 18, 2018. That bill contained a provision that established a deadline for eliminating the use of blood irradiation devices in the United States that rely on cesium chloride by December 31, 2027, through existing voluntary programs, including CIRP, to incentivize the replacement of those cesium chloride blood irradiation devices. This has put a premium on using incentives and other means to accelerate the pace of the program to meet that deadline. In addition, acceleration of CIRP implementation also puts a premium on pivoting the program from its current focus on blood and research irradiators toward other applications, including Sterile Insect Technique (SIT) and industrial irradiators and radioisotopic well-logging devices, applications for which alternative technologies may not be immediately available.

This paper will provide an overview of how CIRP was able to secure volunteer sites to transition to x-ray technology, the kinds of incentives used, how the program was able to address site concerns about the replacement devices, how the program is working toward meeting the 2027 deadline, and the future of CIRP as it applies to other applications beyond blood and research irradiators. In so doing, the paper can provide a useful roadmap for other States to achieve similar permanent risk reduction results.

State

United States

Gender
Primary authors:  Ms LIEBERMAN, Jodi (Sandia National Laboratories);  Dr ITAMURA, Michael (Sandia National Laboratories)

Presenters:  Ms LIEBERMAN, Jodi (Sandia National Laboratories);  Dr ITAMURA, Michael (Sandia National Laboratories)

Track Classification:  CC: Innovative technologies to reduce nuclear security risks and improve cost effectiveness, where feasible
Development of Employee Performance Indicator for Predicting the Insider Threat Behavior

National Nuclear Energy Agency (BATAN) of Indonesia has been implementing trustworthiness assessment for nuclear facility employee which is part of nuclear security culture program. Currently, survey, interview and observation are still the best methods to assess the changes of employee behavior. These methods are become too subjective and difficult to measure and reanalyze due to the involvement of many experts with different knowledge and skill background. Therefore, it is necessary to develop the method for identifying and classifying employee personal behavior and scoring the degree of potential behavior of malicious insider threat. The objectives of this study are to establish the method for predicting the insider threat by measuring employee performance indicators as a function of personal behavior which can be analyzed quantitatively. There are two steps of constructing the employee performance indicators. The first step develops the standard indicator of trust employee behavior based on national standard of civil servant recruitment and the norm in local culture and establishes the psychological questionnaire to measure contradictive behavior which is potential to be insider threat. At the second step, qualitative data from the first step are quantified by scoring each of questionnaire, clustering the data based on the employee behavior and analyzing statistically the scores. These scores are to be compared to standard indicator of trust employee to obtain employee performance index. This index is expected to be able to show a trend of employee behavior which can be analyzed further for predicting the insider threat behavior in trustworthiness program.

State
Indonesia

Gender
Male

Primary authors: MARDHI, Alim (BATAN); Mr ANTARIKSAWAN, Anhar (BATAN); Mr BASUKI, Fatmuans (BATAN); Mr WASKITA, Adhyaksa (BATAN); Mrs RINA S, Geni (BATAN); Mr KHARUL, Khairul (BATAN); Mrs KRISTUTI, Endang (BATAN); Mr SUDILOWAN, Usup (BATAN); Mr ISKANDARSYAYAH, Aulia (Padjajaran University); Mr JUARSA, Mulya (Batan)

Presenter: MARDHI, Alim (BATAN)

Track Classification: PP: Insider threats
Vulnerability Assessment using Modeling and Simulation: Applications and Lessons Learned

Vulnerability Assessment using Modeling and Simulation is a quantitative and performance-based methodology to measure the overall effectiveness of physical protection system. IAEA TECDOC-1868 "Nuclear Security Assessment Methodologies for regulated facilities" addressed M&S in security assessment.

In this presentation, I would like to share our experience in M&S. KINAC, has a regulation role with NSSC (ROK’s regulatory body) in physical protection, have convened a project to model all the nuclear power plant using a software tool AVERT and to performs vulnerability assessments in the Republic of Korea from 2014 to 2019.

First, it is a substantial job to model all the nuclear power plant, which has thousands of physical protection elements, and hundreds of thousands of 3D modeling elements. You have to model building interior/exterior layout, infrastructures and terrain. Old facilities, like Kori-1 nuclear power plant built in 1977, is very difficult get these information, hence many features of modeling should be produced from pictures, rough sketches, and imagination.

Also, this substantial modeling data should be optimized for a reasonable size and analysis speed. At the near end of project, we should modify all the previous modeling to apply our new know-how to optimize modeling.

Second, it is difficult to acquire qualified data libraries of physical protection elements. States with data libraries does not reveal this information because it could show vulnerability of the physical protection elements. Moreover, data of element are not fixed entity. It is interacting other elements and conditions. E.g. the sensing probability of infrared sensors depends on adversary’s penetration methods, tools, skill, weather and delay. If enough delay is provided sensing probability is increases.

To get part of data libraries. we should perform experiments on sensors and barriers in security research, Test and Training facility in INSA/KINAC. To cover other data libraries, we designed and discussed to assign appropriate value and equations. E.g. sensing probability depends on distance and time to stay.

Third, 3D geometric modeling verification problems arises. We have to carefully compare the collected data and modeling results to verify geometric model. A common mistake is that a space is created at the bottom of a fence due to interference with a terrain. Thus the path through this space eventually become shortest cut, usually in curved terrain. In a case, vehicle penetrate inside a protected area through this space.

Fourth, we verified and validated our results of simulation with the Force-On-Force (FOF) exercise. As a regulatory organization, KINAC assesses operator’s FoF exercises, which should be performed once a year at the nuclear power plant site. However, responders and adversaries did not show reasonable move. Because once detected all responders instantly come to adversary, we have to build invisible wall disappearing after some time to simulate the case when responders need time to prepare.

Still, this simulation requires substantial efforts of the specialized expert, even starting from the completed model. Also, the simulation does not guarantee accuracy for the scenario we did not performed, e.g. waterborne attack.

Finally, after several years of stabilization, we got pretty decent modeling having reasonable similarity to FoF exercises. The benefit of M&S is as follows.

1. Very good for the awareness of governmental officers and operators.
2. Very easy to simulate all the other possible scenarios
3. Get confidence on overall effectiveness in PPS
Further we will expand application of M&S from FoF exercises to review of security plans, and inspection on physical protection system.

State
Republic of Korea

Gender
Male

Primary authors: KANG, YEONUK (KINAC (KOREA)); JANG, Sung Soon (KINAC); Ms BAEK, Insun (KINAC)
Presenter: JANG, Sung Soon (KINAC)

Track Classification: PP: Physical protection systems: evaluation and assessment
A simulated Steam Turbine Generator subsystem for Research and Training

This paper proposes an approach to simulate a Steam Turbine Generator subsystem focused on a realistic behavior and architecture of the IT-components with the aim of supporting training for cyber-security operators and cyber-security investigators. The scientific contribution of this paper is a description of the Steam Turbine Generator from a computer scientist point of view, the analysis of requirements for such a simulation and the design of an architecture fulfilling these requirements.

Steam turbines form an integral part of any power plant. They perform the task of generating electric power by using the steam pressure generated by the steam generators of the reactor. In general, steam turbines consist of a shaft connected to a number of blades and various valves. The rows of blades are spaced around the shaft so that applied pressure leads to rotation. The valves control the steam flow to the turbine. These components are the actors in this cyber-physical system. As such, the valves are controlled by ICS (Industrial Control Systems) and might be the target of cyber attacks or affected by transmission errors.

Currently, the possible detection of attacks on the ICS controlling valves within Steam Turbine Generators is barely researched, as well as the mitigation of and recovery from potential attacks. This includes the investigation of potential attacks.

Our proposal is to provide a model and simulator with realistic representation of involved hardware, software and communications architecture of a Steam Turbine Generator system. Modeling this Steam Turbine Generator system requires understanding the system from a computer scientist point of view, including computing units, sensors, actuators and the communication between these components. The simulation requires adherence to a realistic behavior of the software components and communication protocols. In addition, this simulation can trigger a pre-defined ranges of unusual behavior, caused by cyber events, operator error or attrition of components.

In contrast to a physical mock-up or a control room simulator, such a simulation aims at being easy to deploy, easy to alter and easy to scale. It focuses on the IT-components and not only on physical processes. Hence, it can serve as a foundation for a.) research into cyber-security measures like techniques for detecting or mitigating attacks, b.) training platform for cyber-security operators with regards to detection and mitigation of cyber-events, c.) training for cyber-security investigators by allowing investigation into the IT-components and d.) for operators in terms of recovery from a cyber-event caused error within a subsystem.

The simulation proposed in this paper is demonstrated using PLCSIM Advanced to create virtualized PLCs. This allows easy deployment for training purposes. The virtualized PLC communicates (physical) process variables using OPC UA with the simulation module, making this approach more scalable. This simulation module handles the underlying physical process and provides the virtualized PLC with realistic input via the PLCSIM Advanced API. The simulation module is programmed in C# and allows for easy alteration or extension of the system setup. In addition, the simulation module is able to inject various cyber events, errors and jitter to the transmitted data. In addition, a local HMI is included to give a system operators view to a potential trainee or investigator. This architecture allows the researcher access to the ‘physical reality’ of the simulated process as well as the ‘PLC reality’ (how the physical process performs from the viewpoint of the PLC) as well as the ‘Operator reality’ (how the physical process performs from the viewpoint of the Operator).

The final submission will include the architecture of the simulator, a definition of the communication flow, a definition of various fault states and attacks available from the simulator and an
investigation into potential forensic traces within the network communication and the attached PLCs.

State
Germany

Gender
Not Specified

Primary authors: ALTSCHAFSEL, Robert (Otto-von-Guericke Universität Magdeburg); HILDEBRANDT, Mario (Otto-von-Guericke-University of Magdeburg); Prof. DITTMANN, Jana (Otto-von-Guericke-University of Magdeburg)

Presenters: ALTSCHAFSEL, Robert (Otto-von-Guericke Universität Magdeburg); HILDEBRANDT, Mario (Otto-von-Guericke-University of Magdeburg)

Track Classification: CC: Information and computer security considerations for nuclear security
Management of neutron and low-intermediate level gamma Disused Sealed Radioactive Sources (DSRS) (Waste) in Zimbabwe

Main Author
Innocent Mayida imayida@rpaz.co.zw

Co-Authors
Amos Muzongomerwa
Natsai Mutanga
Radiation Protection Authority of Zimbabwe

Sealed radioactive sources have found many uses which improve human activities and the quality of life of people. In Zimbabwe, a lot of sealed radioactive sources are used in the medical, mining, construction and processing industries. These applications generate radioactive waste that may represent safety and security risks to the environment and people. This creates the need to manage the use and after the lifetime of radioactive materials and waste. The radioactive waste including disused sources must be managed well particular care to radiological, biological, chemical and physical hazards.

There is a need to develop a strong radioactive waste management infrastructure from importation, use and final disposition including regulatory requirements, sociopolitical and economic use. The country policy requires that after the lifetime use of the radioactive sources, they are returned back to the country of origin. However, most of the disused sealed sources can’t be sent back to the country of origin, therefore, the country had to develop mechanisms for the management of safety and security before final disposition. This paper describes measures that have been taken by the regulatory body through the help form the International Atomic Energy Agency (IAEA) on managing disused sources in the country. In Zimbabwe, most neutron and low-level gamma sources are used in moisture density measurements for the construction industries. The paper will examine the safety and security risks posed by these disused sealed sources in the developing world where there is minimum radioactive waste management infrastructure or absence thereof. The study will describe the operation procedure, identification of sources, characterization, separation of neutron and gamma sources and measurement of contamination before and after conditioning exercise.

The conditioning process involved twenty-six nuclear moisture gauges (mostly Troxler gauges with fewer other manufacturers). In addition, six Cesium (Cs-173) sealed gamma sources from the radiotherapy were conditioned.

The results will be discussed and presented including suggestions for management of disused sources, new policy approach and development of locally based competence in this regard. Based on measurements and calculations carried out during the conditioning exercise it was found out that radioactive waste management can be met with reasonable costs by implementing a waste management plan using appropriate technologies and expertise fit for developed countries.

State
Zimbabwe

Gender
Male

**Primary author:** Mr MAYIDA, Innocent (Radiation Protection Authority of Zimbabwe)

**Co-authors:** Mr MUZONGOMERWA, Amos (Radiation Protection Authority of Zimbabwe); Ms MUTANGA, Natsai (Radiation Protection Authority of Zimbabwe)

**Presenter:** Mr MAYIDA, Innocent (Radiation Protection Authority of Zimbabwe)

**Track Classification:** PP: Risk-informed approach to the security of radioactive material in use and in storage
Developing the Transportation – Security, Tracking and Reporting System (T-STAR) System

The Transportation – Security, Tracking and Reporting System (T-STAR) was developed by NNSA NA-21 Office of Radiological Security (ORS) to provide a transportation security system for use during transport of Category 1 and Category 2 radiological material to provide detection and tracking capability for shipments. While many off the shelf systems provide asset tracking of the conveyance, few offer detection of a breach into the cargo compartment or the removal of cargo from the conveyance. Systems that do offer such capability need to be permanently installed on the conveyance, requiring drilling of holes and running of cables throughout the conveyance itself. This means that dedicated shipping containers or vehicles are required, and this is not sustainable in many countries where ORS is building capacity for the security of radioactive materials in use, storage, and in transport. T-STAR is leveraging various ORNL technologies for improved communications capability and reduced power requirements; the multimode communications module developed by the Unmanned Aerial Systems group and the low power and extensible Authenticatable Container Tracking System (ACTS) tag developed for the US Department of Energy’s Packaging Certification Program provide a small footprint tracking system which can be installed quickly as needed. T-STAR uses a cellular and an Iridium modem to communicate configuration and alert information to a server used to monitor the shipment and incorporates a Z-wave® wireless security system allowing various intrusion detection sensors to be located in the conveyance. The Z-wave sensors are readily available, inexpensive, and power efficient, making them replaceable and low maintenance. The server software be configured as a standalone system installed on a light duty computer hosted by the competent authority, carrier, or response agency, or hosted as part of an Amazon Cloud Server (AWS) accessible via a secure login. The server has two functions, first is to handle messages to/from the T-STAR field unit, second is to host the user interface which can be accessed using a web browser on desktop or mobile device. The user interface implements roles to determine the level of access to shipment information, define geo-fences, and configure notifications. The user interface also supports multiple languages for display as well as notifications by using a simple lookup file which can be modified by the host country to ensure translations are correct and meaningful to responders receiving notifications and alerts. This paper will detail the overarching T-STAR capabilities, architecture and components, and provide insights on how it is deployed, used, and monitored during transportation of radioactive material.

State

United States

Gender

Male

Primary authors:  Mr SCHULTZE, Michael (Oak Ridge National Laboratory); Mr YOUNKIN, James (Oak Ridge National Laboratory); Mr STINSON, Brad (Oak Ridge National Laboratory); Mr VACALIUC, Bogdan (Oak Ridge National Laboratory); Mr FRANK, Steven (Oak Ridge National Laboratory); Mr
SALESKY, Ron (Oak Ridge National Laboratory); Mr THOMPSON, Thad (Cadre5, LLC); Ms HACKETT, Alexandra (Oak Ridge National Laboratory)

**Presenter:** Mr SCHULTZE, Michael (Oak Ridge National Laboratory)

**Track Classification:** PP: Transport of nuclear and other radioactive material: practices, challenges and regulatory issues
Building Capacity in Member States through Coordinated Research Activities – Increased understanding and performance in nuclear security in Albania

The Institute of Applied Nuclear Physics (IANP) was established in 1970, and is the main user of the radioactive sources in Albania. IANP is a focal point and the main user and provider of nuclear and nuclear related techniques in the country and conducts research, applications, education and expert training in this field. According to Decision No. 563, 22.08.2007 of the Council of Ministers, IANP supports the Albanian Atomic Authority for the promotion of nuclear and related techniques and knowledge in the country.

IANP provides advice and services to the governmental and other institutions related with nuclear applications, radiological emergency response, radioactive waste management, security of nuclear and radiological facilities, combating illicit trafficking of radioactive materials and is the main transporter of radioactive materials and radioactive sources for whole country.

IANP has excellent cooperation with International Atomic Energy Agency through Technical Co-operation programme and Technical Cooperation Department (National, Regional, Interregional Projects) and Coordinated Research Projects (CRP) with Department of Nuclear Safety and Security.

In 2016 IANP joined the CRP J02005 titled “Improved Assessment of Initial Alarms from Radiation Detection Instruments” with Research Contract Title “Collection and Analysis of Radiation Detection Data for Alarming Containers”, and in 2018 joined the CRP J02012 titled “Advancing Radiation Detection Equipment for Detecting Nuclear and Other Radioactive Material out of Regulatory Control” with Research Contract Title “Analysis of Human Engineering Interface with Radiation Detection Equipment’s for determining optimal equipment specifications”.

Participation in the CRP J02005 and the knowledge gained in strengthening the understanding of the performance and assessment of alarms from radiation portal monitors (RPMs), that comprise the backbone of radiation detection system operations in Albania, has been a great support in improving systems (equipment and operations) sustainability. The activities under this CRP consist of obtaining information on radiation alarms (from declared radioactive material shipments, commodities causing an alarm from the presence of radionuclides of natural origin, and other shipments or occupancies of portal monitors) including the physical characteristic of the commodity, the conveyance with the commodity, and the radiation detector data for that commodity. The compilation of data has been instrumental in the development of tool that can assist in the effective, efficient, and consistent assessment of alarms – and with the advantage of sustainable training options. The software tool called TRACE (Tool for Radiation Alarm and Commodity Evaluation) also provides an easy to use reference library for assessing the information associated with a radiation alarm. To better understand the response of the RPMs to potential nuclear security threat and general commerce occupancies, a number of experiments have also been performed. The experiments provided further information on the response of RPMs to alarming commodities under varying circumstances. Arrangements were made to run the same vehicle through multiple RPMs (even at different sites and different speeds) to obtain and compare RPM profiles between different types of detectors and various natural background conditions. The result of these investigations and participation in the CRP activities (including networking and project meetings) has greatly increased Albanian understanding of RPM operations and improved the sustainable use of the systems for nuclear security and facilitation of safe and secure trade. The capacity building outcome of the CRP should be recognized.

IANP is also an active participant in CRP J02012 where the work has been focused on research experiments with different portable radiation detection instruments to perform important human factors studies related to specifications of handheld and backpack-borne radiation detectors. IEC and other standards for radiation detectors provide guidelines for weight and size of instruments
but these are often not compatible with the actual operations the instrument will be used in. As a result, factors such as physical characteristics of the instrument user (age, height, sex, clothing (winter or summer)) have not been previously taken into account. In collaboration with Department of Physics in the Faculty of Natural Sciences, Albania conducted research experiments involving different form factors and weights of instruments against different age, weight, height, and sex of potential users (simulated initially by students and Institute of Applied Nuclear Physics personnel). The research experiments were performed in different weather conditions (winter/summer) classroom and field conditions for determining optimal equipment specifications. These experiments have provided important on the ability of users to actually hold and operate detectors used for nuclear security operations given the weight, size, and form factor of the instrument. This information will support the revision of the IAEA’s Nuclear Security Series 1, Technical and Functional Specifications for Border Monitoring Equipment, and improve the specification and procurement of instruments leading to more sustainable and effective nuclear security detection operations.

Albania has applied also to participate in the new CRP J02014 titled “Advancing Maintenance, Repair and Calibration of Radiation Detection Equipment” with Research Contract Title “Analysis of Radiation Detection Equipment Failures: Causes and Sustainable Maintenance Plans”. This CRP is expected to even further increase the human knowledge and capacity of Albania to better understand performance of Albania’s radiation detection systems and improve sustainability of them. Participation in the CRPs has also provided Albania officials and experts an opportunity to expand professional and nuclear security networks by seeing, participating in, and developing new approaches to implementing effective nuclear security detection operations. Albania enthusiastically recommends continuation of the agency CRP activities and looks forward to further involvement in these important projects. Providing mechanism that enable Member States to jointly solve pressing problems builds capacity and ensures future sustainment of nuclear security systems. The small investment made in supporting research contracts can be easily shown to have huge positive returns.

State
Albania

Gender
Male

Primary author: Prof. BYLYKU, Elida (Institute of Applied Nuclear Physics)

Co-authors: Dr PRIFTI, Dritan (Institute of Applied Nuclear Physics); Dr MASSEY, Charles (International Atomic Energy Agency); Dr DACI, Brunilda (Institute of Applied Nuclear Physics); Dr TUSHE, Kozeta (Institute of Applied Nuclear Physics)

Presenters: Prof. BYLYKU, Elida (Institute of Applied Nuclear Physics); Dr PRIFTI, Dritan (Institute of Applied Nuclear Physics)

Track Classification: MORC: Detection technology development and performance testing
Abstract
Nuclear security is facing great challenges nowadays due to the rapid development of technology, and Drones are one of among the major growing new technology which are currently considered the biggest threat to nuclear facilities, and I focused in these study on a type of Drones called small Unmanned Aerial Vehicles where it became spreading at everywhere, have many commercial applications, and anyone can easy own it.

These Paper addressed the potential threats, risks and the impact of the widespread use of Drones and the impact of these spreading to the security of nuclear facilities. Threats will clearly differ from country to country, region to region and location to location but I focused on the middle east area to show several examples of using Drones by terrorists for attacking facilities and individuals in Iraq and Syria. And these sure that terrorists and any one have malicious intents may be using Drones for attacking Nuclear Facilities in the near future and there is not nuclear security system currently have anti_drones to prevent the expected Drones attacks

In these study I took in my consideration International Atomic Energy Authority nuclear security recommendations when I introduced sum of solutions and suggests to mitigate the threats of Drones, by improvement the current legislation which regulate the use of Drone, and the imposition of sanctions on those who violate the law of their use, and enhancement Nuclear Security System to prevent, detect, delay, and response (neutralization) of Drones attacks at nuclear facilities on time and upgrading physical protection systems for all nuclear and radio-logical nuclear facilities.

It will a revolution in the manufacture of the Drones during the next five years and the Drones will develop fast and have a big capability to arrive long distance, carry explosive materials and it will have advanced artificial intelligence systems help it to do tasks at any time, so that, we should build strong nuclear security systems flexible to be able to for facing the expected threats of Drones in the near future.

Keywords: nuclear security, Drones, Threats, Risks. Unmanned Aerial Vehicle

State
Egypt

Gender
Male

Primary author: Mr ALLAM, Mohammed (Egyptian)

Presenter: Mr ALLAM, Mohammed (Egyptian)
Session Classification:  Risks and benefits to nuclear security from innovations in other fields, including artificial intelligence and big data

Track Classification:  CC: Risks and benefits to nuclear security from innovations in other fields, including artificial intelligence and big data
DEVELOPMENT OF OPERATIONAL POLICY IN NUCLEAR MEDICINE SERVICES FOR THE MINISTRY OF HEALTH MALAYSIA: SECURITY OF RADIOACTIVE MATERIAL

BACKGROUND

In Malaysia, the Ministry of Health played a very important role to ensure the safety and security of radioactive material used in medicine particularly in nuclear medicine. The mechanism of the controlled was set by the implementation of the regulatory requirements such as registration and registry requirements, monitoring, and enforcement as well as prosecution practice. These elements were according to the standard set by the Director General of Health through embarking the new policy document called the Operational Policy in Nuclear Medicine Services. The document which has been produced was the operational requirements according to the Atomic Energy Licensing (Basic Safety Radiation Protection) Regulations 2010 (the subsidiary regulations under the Atomic Energy Licensing Act 1984).

The security of radioactive materials was taken into consideration where the specific chapter of the document was meant for the security aspect. From the order, purchase, transportation, radioactive waste management as well as management of theft, loss or sabotage of radioactive source used also highlighted and covered in this document. The topics of the chapter are designed through the special Task Force formed under the Drafting Committee of the Nuclear Medicine Services, Malaysia Ministry of Health.

The paper aimed to describe the commitment of the government of Malaysia particularly the Ministry of Health (MOH) and its institution such as hospitals to initiate and designed the policy dedicated for the security of radioactive material used in nuclear medicine services.

METHODS

The Malaysian’s MOH has developed the document based on the needs of the latest requirements under the Atomic Energy Licensing (Basic Safety Radiation Protection) Regulations 2010. This is the subsidiary regulations under the Act 304. The topics of the chapter are designed through the special Task Force formed under the Drafting Committee of the Nuclear Medicine Services, Malaysia Ministry of Health.

RESULTS

The medical institutions especially the facilities involved in radioactive used for medical purpose have applied good practice according to this document. The policy of the management of theft, loss or sabotage of radioactive source is very important and these guidelines are in-line with requirement stipulated under the Atomic Energy Licensing (Basic Safety Radiation Protection) Regulations 2010. The policy quoted ‘upon discovering of any theft, loss or sabotage of any radiation source in his possession or under his control, the licensee has to notify the appropriate authorities (e.g. police, fire & rescue department, etc.) and in all cases, the licensee / Nuclear Medicine physician / RPO shall notify the MRSD / AELB of the accident within 24 hours; confirm in writing within 48 hours, investigated with necessary corrective measures taken and submit a complete report of the accident within 30 days after notifications to the appropriate authority’.

Radioactive source security should be of concern to the leadership (board members and executive management) of a healthcare facility because they are the ones who would bear the ultimate liability should one or more of the radioactive sources used in their facility be lost, stolen or sabotaged and result in harm to people and/or the environment. Even a minor security incident could generate widespread public panic, make the facility’s radioactive sources temporarily unavailable, and seriously impact the patient population that the facility serves.
CONCLUSIONS

In the interest of public safety and national security, the potential hazards of using radioactive source on the patients and the associated radiation risks to staff, public and the environment should be kept in mind. All personnel shall comply with the laws, regulations, local rules and the radiation protection guidelines set by the department.

Based on this document, the Policy Makers encompasses of the Top Management and Regulators as well as the medical institution could consider enhancing the content of developing a common standard for incident reporting that requires reporting Category 1 and 2 losses; encourage wider reporting transparency, Improve physical security measures; expand electronic tracking of dangerous radioactive sources, Improve security culture and Encourage material replacement efforts.

State

Malaysia

Gender

Male

Primary author:  SAUFI, SYARUL IMAN (MINISTRY OF HEALTH)

Co-author:  Dr NG, Chen Siew

Presenter:  SAUFI, SYARUL IMAN (MINISTRY OF HEALTH)

Track Classification:  CC: Implementation of national legislative and regulatory frameworks, and international instruments
Development and Application of China Customs Radiation Detection Integrated System

China Customs began developing the integrated system of fixed radiation detection equipment in 2018, and put it into trial operation in early 2019. In 2019, more than 3,000 sets of fixed equipment will be integrated. The integrated system of radiation detection equipment transmits the alarm data, images and equipment status information scattered at ports nationwide to all directly affiliated customs and the management terminal of the General Administration of China Customs, providing auxiliary law enforcement basis for subsequent disposal or issuing instructions. This paper comprehensively introduces the application of China Customs Radiation Detection Integrated System in customs work from the aspects of equipment integration and data collection, data transmission processing and distribution, radiation detection link management, statistical analysis and panoramic display, equipment management and efficiency evaluation, system management and so on. This paper discusses the difficulties and solutions in the system deployment process and summarizes the mature experience in radiation detection management of China Customs.

State
China

Gender

Primary authors: Mr HOU, Yongming (China Customs); Ms LIU, Xinxia (China Customs)
Presenter: Ms LIU, Xinxia (China Customs)

Track Classification: MORC: Building and maintaining nuclear security detection architecture
Nuclear Security Measures to Address Best Practices Associated with Nuclear/Radiological Threats for Major Public Events

Abstract

The U.S. Department of Energy/National Nuclear Security Administration (DOE/NNSA), International Atomic Energy Agency (IAEA), U.S. Department of State (DOS), and the Panamanian Chemical, Biological, Radiological and Nuclear (CBRN) response teams unified and coordinated an approach that demonstrated best practices for nuclear security measures for Major Public Events (MPEs), as outlined in IAEA Nuclear Security Series 18 (NSS-18), at the World Youth Day 2019 in Panama City, Panama during January 22-27, 2019. This paper will outline the key factors which resulted in a successful safe and secure event with no radiological or nuclear incidents.

Introduction

Major Public Events (MPEs) are challenging environments in which to conduct nuclear security measures. Many of these events are conducted at the national level and involve long lead time planning efforts and cooperation among a large number of local, state, and federal agencies. The country hosting the events works on national planning guidance specifically for these types of event. These events typically also have international interest whether through attendance by participants from many countries, including heads of state, to high profile television and media coverage. Examples of high profile MPEs include sporting events, such as the Olympic Games and World Cup Competitions, and political/economic events such as the G20 and ASEAN Summits. With extensive international media coverage, these high profile MPEs provide an attractive target for radiological/nuclear terrorism or criminal act. Although the radiological/nuclear threat risk at MPEs is typically low, the economic and political consequences of such an incident would be catastrophic.

World Youth Day 2019

Panama executed their new national concept for emergency preparedness and response associated with major public events by operationalizing an interagency team to manage CBRN prevention and response, and integrating specialists and equipment from DOE/NNSA, DOS, and IAEA. Panama’s response teams demonstrated best practices for interagency coordination and ensured advanced capabilities were in place to prevent, counter, and respond to nuclear/radiological terrorism threats. Their unified approach enhanced coordination between civilian and military organizations, and ensured the teams were prepared to meet the nuclear security requirements for the event.

The coordinated effort was organized under a nuclear security plan that addressed security for potential threats and the capability to respond to terrorist incidents or criminal acts. The Panamanian response team CBRN, coordinated its functions within the Task Force “San Miguel Arcángel (FTC-SMA)”, a group established by the country including all the security sections. With this mechanism, knowledge, technological resources exchanged, preparatory exercises were carried out to acquire the experience to face this highly complex event in the event of radiological incidents.

Response teams and security personnel conducted pre-event baseline surveys of the venues to ensure no radiological or nuclear materials were present. Once the venues were surveyed and deemed clear, they were locked down with strict access controls. Those attending the events were screened for radiological and nuclear materials at the pedestrian and vehicle security entrances. In addition, CBRN expert teams were on standby to rapidly respond in case of an incident.

CBRN security measures in the planning of an important public event is a complex task that requires a high degree of coordination and collaboration. The international community through the DOE/NNSA, IAEA, and DOS provided radiological/nuclear emergency response training to Panama radiation and security experts prior to the event. This training provided practical field op-
Nuclear Security Measures to Add... operations using best practices and detection equipment to survey the venue facilities, parking areas, and roadways around the venue for radiological and nuclear materials. To enhance the CBRN team resources, additional radiation detection equipment was provided to ensure the nuclear security measures could be implemented at all of events and venues.

Summary

The Panamanian CBRN response teams along with U.S. DOE/NNSA, IAEA, and U.S. DOS formed a unified command organization and coordinated an approach for MPE best practices as outlined in NSS-18 at the World Youth Day in Panama City, Panama, January 22-27, 2019. The coordinated efforts and the implementation of national plans and best practices resulted in a safe and secure event with no radiological or nuclear incidents.

State

Panama

Gender

Male

Primary authors:  Mr BUNTMAN, Steven (U.S. Department of Energy); Dr MAURER, Richard (U.S. Department of Energy/National Nuclear Security Administration, Mission Support and Test Services, LLC, Remote Sensing Laboratory, ); Mrs WHITE, Shaleen (U.S. Department of State, Embassy Panama City)

Presenter:  BENSON, Nadja

Track Classification:  MORC: Nuclear security as part of the security of major public events
Safety and Security in shipment of spent nuclear fuel from a research reactor

The MTR type Spent Nuclear Fuel (SNF) assemblies used in the GRR-1 research reactor at National Centre for Scientific Research Demokritos (NCSD), Greece, were repatriated to the United States under the US Foreign Research Reactor Spent Nuclear Fuel acceptance program. The operation comprised packaging and transportation of the SNF from NCSD to the US Department of Energy, Savannah River Site. The project was performed using a NAC-LWT cask along with a lifting yoke, dry transfer system and cask drying and testing equipment. The cask and equipment were packaged in 3 ISO containers and transported by road from NCSD to the Port of Piraeus, maritime from Piraeus to a military port at the US via Portugal and by road to Savannah River Site. The maritime transport was performed using a certified INF3 chartered vessel.

The identification and procurement of the appropriate transport package was performed in full compliance with the safety regulations for the transport of radioactive material that specify, inter alia, package design and test requirements. The carriers and the transport means were contracted, taking into account commercial criteria, along with their technical expertise and experience. The transport program and plan included project management, management systems, emergency preparedness and response arrangements, security means and arrangements. In particular, significant attention was given to the coordination and collaborative efforts performed between the staff of the NCSD, the Greek Atomic Energy Commission (EEAE) and the Department of Energy (DOE), including NNSA Washington DC and Savannah River Site personnel, as well as, the contractors from the US and Greece. The well designed and cautious pre-shipment planning, and the smooth collaboration of the pertinent competent authorities, facilitated the operator in developing an understanding of how to fully comply with both sides of the regulatory framework (safety and security). Moreover, the transport safety-security interface issues were identified as early priority in an effort to evaluate and resolve any challenge in a timely manner.

Apart from broadly implemented SNF shipments’ features, such as, efforts to avoid catching public attention, specific attention was given to the management of sensitive, security-related information, which was disclosed only on a “need to know” basis. It worth mentioning that the experience gained in the country during the previous SNF shipment in 2005 proved a significant asset, in facilitating the organization and the successful completion of the recent SNF shipment. This paper gives an overview of the activities implemented for the SNF transport and the challenges encountered for the safe and secure completion of the shipment. It describes the main activities related to the secure and safe shipment performance, including the description of the pre-shipment planning and coordination activities which were a key to the success of the project.

State

Greece

Gender

Female
Primary authors: Mrs VOGIATZI, Stavroula (Greek Atomic Energy Commission); Dr STAMATE-LATOS, Ion (National Centre for Scientific Research "Demokritos")

Co-author: Dr NOUNESIS, Georgios (National Centre for Scientific Research "Demokritos")

Presenter: Mrs VOGIATZI, Stavroula (Greek Atomic Energy Commission)

Track Classification: PP: Transport of nuclear and other radioactive material: practices, challenges and regulatory issues
Toward a Localized Cybersecurity Strategy for Critical Assets

Monday, 10 February 2020 11:45 (15 minutes)

The quantity and capability of cyber-attacks targeting Industrial Control System (ICSs) is growing rapidly. The integration of digital technology and communication channels in Nuclear Power Plants (NPPs) introduces vulnerabilities to cyber-attacks that may threaten the safety and operation of nuclear power facilities. Current efforts in developing and deploying cybersecurity solutions have focused largely on intrusion prevention, but focus is now turning toward detecting cyber-attacks and ICS intrusions.

Assuming that Intrusion Detection Systems (IDSs) based on host system and network data fail to detect the evidence of a cyber-attack, detection models based on process data (sensor data and control data) can detect deviations from normal operation, which could be a potential cyber-attack. However, most of these process data-based IDSs focus on detecting abnormal signals based on the relationship between the various signals measured by different types of sensors in NPPs. Therefore, these models are unable to detect cyber-attacks where the attacker intelligently tampers with most or all of the signals used in an analysis; if the attacker can tamper with one signal, it is reasonable that they can also tamper other signals simultaneously. In a replay attack, for example, an attacker masks the malicious activity by replaying older measurements. This paper proposes a localized cybersecurity strategy to address cyber-attack detection under scenarios where the sensors are compromised. This proposed strategy excludes the measurements that may be compromised.

The proposed strategy integrates a Kalman Filter into the controller itself to use the command it issued at time t and the state values at time t−1 to predict the expected response of the state values of t+1. This expected response is compared with measurements at t+1; deviations between these values that are greater than a threshold are considered anomalous and potentially caused by a cyber-attack. A Hardware-In-the-Loop (HIL) testbed, which consists of an NPP simulator and a Programmable Logic Controller (PLC), was built to evaluate the effectiveness of the proposed method. The PLC is programmed to control the Steam Generator (SG) water level at the desired set point, by adjusting the feedwater pump speed. A false data injection attack was launched towards the PLC, in which the attacker altered the SG water level measurement using a Man-In-The-Middle (MITM) attack. The altered water level measurement received by the PLC shows that the water level is higher than the set point, which leads the PLC to output commands to lower the feedwater pump speed and subsequently the measured water level. Assuming that the attacker tampered with the SG water level measurement at time t, the model implemented in the controller takes the command issued at time t, which is not compromised, and the state values at time t−1 as inputs, to predict the expected state values at time t+1. By comparing the expected value and the measurements of the state values, which are tampered by attacker at time t+1, the anomaly may be detected. The results of the Kalman Filter implemented in the PLC will be presented in the full paper.

State
United States

Gender
Female

**Primary authors:** Ms ZHANG, Fan (University of Tennessee-Knoxville); Prof. COBLE, Jamie (University of Tennessee-Knoxville); Mr ALLISON, David (AIT Austrian Institute of Technology); Dr SMITH, Paul (AIT Austrian Institute of Technology); Prof. BUSQUIM, Rodney (University of Sao Paulo)

**Presenter:** Ms ZHANG, Fan (University of Tennessee-Knoxville)

**Session Classification:** IAEA Coordinated Research Programmes for Information and Computer Security

**Track Classification:** CC: Information and computer security considerations for nuclear security
Nuclear Security Regulations in Malawi

Effective implementation of nuclear security in a country requires a proper regulatory framework to be in place. Regulations makes an important element of the regulatory framework. Regulations provides requirements to be followed by users to achieve nuclear security.

This paper therefore aims at exploring the efforts being taken in Malawi in ensuring nuclear security regulations are in place. The paper also brings to light the challenges, opportunities and progress in developing and implementation of nuclear security regulations in Malawi.

State
Malawi

Gender
Male

Primary author: GAMULANI, Chimwemwe (Atomic Energy Regulatory Authority)
Presenter: GAMULANI, Chimwemwe (Atomic Energy Regulatory Authority)

Track Classification: CC: National nuclear security regulations
Nuclear security as part of the security of major public events The G20 experience in Argentina

The IAEA defines a major public event as a sporting contest or high level political meeting that presents unique security challenges for the responsible organizations. These kind of events are important because any kind of security problems in them can lead to severe health, social, psychological, economic, political and environmental consequences. The security of a major public event also requires a detailed planning as well as systematic preparation and effective implementation. Decision makers should take into account that sometimes these events are organized by private actor and this fact may have consequences when organizing nuclear security.

Following the idea of the challenges that involve organizing a major public event, thinking a nuclear security operative in these kind of events is also a challenge. Nuclear material used with malicious intentions in a public place could be the following: a radiological exposure device (RED) in a public place, a dispersal of nuclear or other radioactive material (such as a radiological dispersal device –RDD-); a deliberate act to contaminate food or water supplies with radioactive materials, among others. Therefore, for a major public event, the nuclear security system should be an integral part of a bigger security plan for the event and it should also be linked to the nuclear security regime of that State.

On this regard, we should also consider that Argentina is a nuclear country. It has three Nuclear Power Plants (NPPs) in operation and several research reactors spread all over the country. Its nuclear development involves the whole nuclear cycle and it has a mature industry that has built its expertise around it. From a political point of view, nuclear energy in Argentina depends on several actors. From one hand, the independent regulator ARN (Nuclear Regulatory Authority) that has direct link to the Chief of Staff. On the other the Secretariat of Energy that has under its domain the two main operators CNEA (National Atomic Energy Commission) and NA-SA S.A (Nucleoeléctrica Argentina S.A) that are the ones in charge of the research reactors and the operation of the NPPs, respectively. Regarding nuclear security, although the ARN has the enforcement power in terms on regulatory norms, the Ministry of Security is responsible for protecting the civilians and the nuclear facilities. It does it through its four federal forces, the National Gendarmerie, the Federal Police, the Argentinian Prefectura and the Airforce Police.

Regarding nuclear security, in 2018 Argentina held the G-20. This is one of the most important political events in the world where the most important States set goals, agreements and cooperation between them and put some light into the future of the world. All through the year Argentina hosted more than 80 meetings from ministers, diplomats and different senior level politicians. Nevertheless the most important event was the Leaders Summit meeting on November 30th and December 1st. During those days, 38 head of States visited Argentina and held meetings in the City of Buenos Aires. Several major streets and avenues were blocked during both days and the city declared holiday in order to avoid traffic jam and preserve civilians for plausible conflicts during the riots that were programmed for those dates. As it was stated before, nuclear security was part of a bigger security operative and involved several actors in the field.

In light of this event, this paper will describe the challenges Argentina faced in order to conduct the security for that major public event. Those challenges can be well differentiated into three categories. The first one is related to coordination between technical experts and law enforcement agents in the field. The second deals with detection capabilities, how to organize them and how to conduct detection in large areas. Lastly, the third one is connected to updating and preparing protocols of emergency and response in large scale situations.
State

Argentina

Gender

Male

Primary author:  Mr DELUCHI, Facundo (Undersecretariat of Nuclear Energy)

Co-authors:  Mr GADANO, Julian (Undersecretariat of Nuclear Energy);  BIEDA, Tomas (Ministry of Energy and Mining)

Presenters:  Mr DELUCHI, Facundo (Undersecretariat of Nuclear Energy);  Mr GADANO, Julian (Undersecretariat of Nuclear Energy);  BIEDA, Tomas (Ministry of Energy and Mining)

Track Classification:  MORC: Nuclear security as part of the security of major public events
Development of Metrics and Requirements to Enable Downselection and Evaluation of Commercial Counter-UAS Products

Recent security events involving unmanned aircraft systems (UAS) or Remotely Piloted Aircraft Systems (RPAS) have left many Nuclear Sites wondering if they should implement counter-UAS technologies. Many sites are therefore beginning to assess the security risks and potential impact of UAS threats on security, operations, to determine whether implementing Counter-UAS technology or products is warranted. If the assessments indicate unacceptable levels of risk, operators have a challenging task of determining what kind of CUAS capabilities to select and implement, and how to conduct testing to evaluate product specifications and claims made by manufacturers. For operators or regulators seeking to incorporate counter-UAS capabilities into their security systems, a critical next step is to generate requirements based on risk, policy, threat and performance trade-offs. This activity is independent of and must be completed prior to searching for or deploying a CUAS technology. Doing so enables more effective technical exchanges, requests for information, development of test plans and procedures, and provides a solid basis for justifying procurements actions. This is best done through multiple discussions involving all security stakeholders, on topics such as:

• What is the anticipated budget for acquisition and deployment, and annual training, operation, maintenance and sustainment, performance testing, and updates?
• What UAS characteristics (type, navigation methods, size, speed, altitude, payloads, behaviors, etc.) were used to determine unacceptable levels of security risk from UAS threats?
• What unmanned aircraft system behaviors or actions will warrant a response or mitigation action from the Counter-UAS technology?
• What physical areas or airspace boundaries, if crossed by a UAS, would be deemed a security threat?
• How far away must the UAS threats be sensed, assessed (to determine whether a true or nuisance alarm), and mitigated, and at what levels of performance and confidence?
• What forms of sensing and tracking are preferred given local environment conditions?
• What kinds of mitigations are acceptable, legal, and effective given local conditions?
• What are the rules of engagement, and are these acceptable from a policy and legal perspective?
• Who will operate the system, how will notifications and alerts be received and assessed, and what is the process for reporting incidents and actions taken?
• Will the system operate in a stand-alone mode, or be integrated into the rest of the security system?
• What approvals will be necessary prior to operating the system?

The results of these discussions will enable development of requirements and metrics that can be used to evaluate the performance of Counter-UAS regardless of the type of technology being considered. This paper will suggest and discuss multiple performance metrics that can be applied to CUAS at nuclear sites. The metrics presented are based on an established methodology that has been applied to detection and neutralization of threats to high security applications for over 40 years. The Performance Metrics feed into an analysis methodology to estimate security effectiveness of CUAS. Creation of CUAS Requirements will build from performance metrics, resulting analysis, and the amount of security risks and non-security risks decision makers are willing to accept. Recommendations presented in this paper are the result of our combined experience in generating metrics and requirements for CUAS based on security risk, policy, legal, and threat trade space, to form a solid foundation for CUAS down-selection and performance testing.
ernment retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes. – SAND2019-6122 A

State
United States

Gender
Male

Primary author:  Mr BROOKS, Scott (Sandia National Laboratories)
Presenter:  Mr BROOKS, Scott (Sandia National Laboratories)

Track Classification:  PP: Nuclear security of nuclear fuel cycle facilities: emerging technologies and associated challenges and complex threats
Design of the Physical Protection Training Laboratory: Strengthening Effort to Sustain Nuclear Security Capacity Building, BATAN’s Experiences

Teguh Asmoro1, Khairul Khairul2, Fatmuanis3, Naoko Noro4
1 Center for Informatics and Nuclear Strategic Zone Utilization BATAN, Serpong Nuclear Research Complex, PUSPIPTEK Area, Serpong 15314, Tangerang-Indonesia, teguhasm@batan.go.id
2 Center for Informatics and Nuclear Strategic Zone Utilization BATAN, Serpong Nuclear Research Complex, PUSPIPTEK Area, Serpong 15314, Tangerang-Indonesia, khairul@batan.go.id
3 Center for Education and Training, BATAN, Jl. Lebak Bulus Raya, Pasar Jumat, Indonesia, fatmuanis@batan.go.id
4 Integrated Support Center for Nuclear Nonproliferation and Nuclear Security/Japan Atomic Energy Agency, Japan, noro.naoko@jaea.go.jp

Abstract
National Nuclear Energy Agency (BATAN), has the commitment to apply nuclear security in accordance with the requirements set in the Amendment to Convention of Physical of Nuclear Material and Physical Protection and Code of Conduct of Safety and Security of Radioactive Source. In order to develop nuclear security capacity building focus on human resources, based on BATAN Chair Regulation 14/2013, The Center for Education and Training (CET) has the duty to perform education and training, especially in the field of nuclear science and technology including nuclear security. In developing the nuclear security program requires infrastructure in the form of competent human resources, competence based training program and also the adequate training facilities and laboratory that meet IAEA program through Nuclear Security Support Center (NSSC) in order to strengthen nuclear security that is sustainable.

BATAN in cooperation with IAEA, US DOE, ISCN/JAEA in developing a nuclear security program to improve the human resources competence until advance level through regional and international training that organized internally and overseas. Nuclear security in BATAN is a responsibility of Bureau for Legal, Public Relations and Cooperation (BHHK) and supported by technical nuclear facilities while CET is responsible for organizing the training program to fulfill the human resources competence. In addition, CET also has implemented a regional training program with instructors have national and international experience. The cooperation with the Integrated Support Center for Nuclear Nonproliferation and Nuclear Security of Japan Atomic Energy Agency (ISCN/JAEA) for capacity building of Indonesia including BATAN CET began in 2015, and this bilateral cooperation includes ISCN/JAEA assistance for designing and implementing Physical Protection Training Laboratory at CET.

In developing nuclear security capacity building BATAN still has a constraint in providing a laboratory facility to perform the exercise. Physical protection laboratory consists of mock up facility and its physical protection system, detection system lab, delay system lab, assessment system lab, support system maintenance lab, Detection lab for secondary check and Integrated System of PP. This paper will also describe Indonesia-ISCN/JAEA cooperation program and its achievements, and it serve as a good reference of collaboration among training centers.

Keyword: Human Resources, Training, detection, Delay, Assessment, training tool

State
Indonesia

Gender

May 9, 2020
Male

**Primary author:** Mr KHAILRL, Khairul (BATAN)

**Presenter:** Mr KHAILRL, Khairul (BATAN)

**Track Classification:** CC: Role of Nuclear Security Support Centers to support and sustain national nuclear security regimes
Industry Engagement to Establish a Robust Security Approach to Mobile Radiological Sources

The U.S. Department of Energy/National Nuclear Security Administration’s Office of Radiological Security (ORS) collaborates with partner countries across the world to enhance the security of radioactive sources that are used for legitimate purposes. Defining and implementing a robust security approach across any industry that uses radioactive material requires strong coordination with multiple stakeholders. In the case of mobile radioactive sources, such as those used in the oil, gas, and geo-physical industries (also referred to as the well-logging and radiography industries), the fact that the sources move through various operational and regulatory jurisdictions increases the number of stakeholders and makes security more challenging. Success depends on the ability to look at the operational use holistically, identify the stakeholders that would be involved if a source was lost or stolen, and identify roles and responsibilities of these stakeholders to accommodate proper notification, adjudication and response to a security incident.

The mobile radiological sources used in the well-logging and radiography industries are of sufficient curie quantities to be categorized as desirable material for malicious actors. Beyond the security risk posed by these sources, there is also an understanding of the potential damage, both reputational and monetary, that a lost source would have on the licensee and the industry overall. Identifying and communicating the risk these sources pose with impacted stakeholders is a critical first step in developing a security approach.

Common day-to-day operations within both industries drive the unique security challenge of mobile sources. From storage facilities, transportation vehicles, temporary storage locations, and use in the field, each phase creates challenges regarding source control and accountability. All aspects of the operational use of these sources needs to be fully understood in order to address security equipment enhancements, policies, procedures, and training.

This paper will leverage more than ten (10) years of experience that ORS has gained working closely with industry partners and mobile radiological source users across the well-logging and radiography industries. It will identify the risk posed by mobile radiological sources, clearly define the operational phases of each industry, identify security best practices of mobile sources, and discuss what long-term, sustainable security looks like within these industries. In addition, it will explore areas of a robust security approach that are not commonly given priority in these industries, such as alarm adjudication and response.

State

United States

Gender

Male

Primary author: KLUSE, Blake (Office of Radiological Security/Pacific Northwest National Laboratory)

Co-authors: Mr CARR, Michael (Pacific Northwest National Laboratory); Mr ANDERSON, Gerald
(Pacific Northwest National Laboratory)

**Presenter:**  KLUSE, Blake (Office of Radiological Security/Pacific Northwest National Laboratory)

**Track Classification:**  PP: Transport of nuclear and other radioactive material: practices, challenges and regulatory issues
Surveillance using unattended transmission: A powerful control tool for enhancing nuclear security

Padmakumar Sankaran Nair, Ranajit Kumar and Agrawal S.K
Nuclear Controls and Planning Wing, Department of Atomic Energy, India
Email: padmakumar@dae.gov.in, padma.kumar@gov.in

Abstract

Nuclear material accounting in any nuclear installation is an important tool to ensure that the nuclear material (NM) inventory is maintained on a regular basis and thereby detecting unauthorised removal at the earliest. In general, the Agency verifies the accounting reports at a specific frequency, and the physical verification is done annually. Any discrepancy in actual inventory or the monthly declarations submitted by member states could thus be detected only during these periods. Unattended transmission of information from nuclear facility to the Agency headquarters may be a better option for detecting discrepancies if any, resulting in enhanced nuclear security. Nuclear material surveillance methodologies include equipment used to monitor nuclear material and its associated equipment. The technical measures used should be capable of providing near real-time alarms to indicate failure of surveillance itself or that of the material control measures under surveillance. This information can be made available to both the facility operator / State as well as the Agency at any desired time frequency including the scope for near-real time provision. In this context, India’s experience in providing remote data transmission from one of its facilities to the IAEA enabling strengthening of nuclear security is shared in this paper.

One of India’s nuclear facilities is being monitored remotely by the Agency though unattended data transmission methodology and the efficacy of this system has been demonstrated very effectively. The usual physical inspection frequency to this facility prior to the remote data transmission regime was once in a month. At present, the data is collected on a daily basis and remotely sent to the Agency headquarters. The frequency of data collection is software controlled and could be further increased even to near real time also, if required. This technology not only improves the verification efficiency, but reduces the inspection efforts as well, including cost reduction.

The remote data transmission deployed in India by the Agency is based on surveillance of electronic seal information, transmitted to the Agency headquarters through a secure Virtual Private Network (VPN) connection using the public internet services. The security of data is ensured using hardware encryption modules provided by the Agency deployed both at transmission as well as receiving end. Data (seal information) is collected at every day at 00:00 hrs in a programmed manner. Extending this remote data transmission technology to other area for improving verification efficiency and thereby contributing to nuclear security is addressed in this paper.

References:

2. INFCIRC/225/Rev.5: IAEA Recommendations.
3. Use of nuclear material accounting and control for nuclear security, IAEA NSS series 25-G
4. Establishing a system for control of nuclear material for nuclear security purposes at a facility during use, storage & movement, IAEA NSS series, 32-T
Gender

Male

Primary author:  Mr PADMUKUMAR, S (Scientific Officer)

Co-authors:  Mr KUMAR, Ranajit (Scientific Officer); Mr AGRAWAL, Surendra (Scientific Officer G)

Presenter:  Mr PADMUKUMAR, S (Scientific Officer)

Track Classification:  PP: Nuclear material accounting and control
POLAND: A COMPREHENSIVE APPROACH TO CESIUM SECURITY

The U.S. Department of Energy’s Office of Radiological Security (ORS) cooperates with partner countries throughout the world to enhance the security of radioactive sources used for legitimate purposes. A large number of these sources are within hospitals, universities and other public establishments. High activity Cesium-137 is one of the primary isotopes used to irradiate blood for the prevention of Transfusion Associated Graft versus Host disease (TA-GvHD). As member states continue to intensify their support for the implementation of the IAEA security recommendations in Nuclear Security Series No. 11, Security of Radioactive Sources, operators face a growing strain on their security resources in both financial and human capital terms. ORS is pursuing a Global Cesium Security Initiative (GCSI) that focuses on enhancing physical protection of cesium irradiators.

In the course of discussions with partners, there is an emerging interest in strategies that enable the permanent reduction of the risks associated with Cesium-137. Although several countries, including France, Norway, the U.S. and Japan have pursued these strategies and moved towards X-ray as a non-ionizing technology to achieve critical service provision, there still has been limited adoption of X-ray internationally for these uses until more recently. In Poland, for example, a number of regional blood centers and hospitals have declared their intention to switch from Cs-137 to X-ray. The adoption of X-ray by the first Polish site is fairly new, but through the GCSI, ORS is working to transition at least six volunteer sites by 2020 from cesium-based irradiation to X-ray based blood irradiation. This momentum can be attributed in part to the age of the cesium devices and the procurement decision timeframe, but also the ability of the regulator to discuss the full cost of ownership for radio isotopic devices, such as security systems and disposition costs. The paper will highlight how technical exchanges among the Polish regulatory authority, waste management organization (ZUOP), radiological facilities and various subject matter experts (SMEs) created synergy to drive the risk reduction conversation. The costs associated with the security of radioactive sources can be significant. As regulators begin to enact legislation that requires sites to ensure the safe and secure disposal of old cesium based irradiators, and as sites consider the costs of potential liability that may arise from a malicious act involving radioactive sources, they have begun to realize the true cost of securing cesium for use, rather than exploring other methods such as X-ray based irradiation.

In the case of Poland, radioactive sources licensees must provide financial resources in the form of an “escrow” to ensure the safe and secure disposition of disused sources at end of life. The focus on enhancing security regulations and lifecycle management of radioactive sources, coupled with technical exchanges, is leading licensees to evaluate the complete cost of ownership and operation of radioisotopic devices. The paper will identify the challenges, best practices, and lessons to be learned from Poland’s experience grappling with the challenges of securing cesium-137 when the issue is considered holistically.

State
United States

Gender
Female
Primary author: ELSTER, Jennifer (PNNL)

Co-authors: Mr JAMISON, Jeremy (Pacific Northwest National Laboratory); MORRIS, Frederic (Pacific Northwest National Laboratory); Mr DZIKOWSKI, Bartosz (Radioactive Waste Management Plant ZUOP)

Presenter: ELSTER, Jennifer (PNNL)

Track Classification: PP: Risk-informed approach to the security of radioactive material in use and in storage
Improving Trace Element “Fingerprinting” of Uranium Ore Concentrates

The Canadian Nuclear Safety Commission (CNSC) Laboratory, working within the Nuclear Material Signature and Provenance Assessment Capability Development Project (NMS/PAC), has developed a laser ablation inductively coupled plasma mass spectrometry (LA-ICP-MS) method for rapid bulk trace element analysis of uranium ore concentrate (UOC) suitable for both national nuclear forensics library (NNFL) maintenance and analysis of intercepted nuclear forensics samples (1). The method enables rapid, accurate and precise trace element analysis of UOC with almost no radioactive waste generated and minimal sample consumption, which is ideal for nuclear forensics.

The LA-ICP-MS method provides a measurement of 48 element concentrations. Limits of quantification range from $1.7 \times 10^{-7}$ to $2 \times 10^{-3}$ mg/mg Uranium, reflective of uncertainties that vary depending on the measured element. The applicability of LA-ICP-MS in attribution of UOCs was tested by performing a provenance assessment exercise using a selection of 28 samples comprising:

1. Three standard reference UOC samples obtained from the International Atomic Energy Agency (IAEA): IAEA8745, from Olympic Dam; IAEA8747, from Ranger mine; and IAEA 9449, an artificial sample made of a mixture of an old CRM and UOC from the Rössing mine,
2. 22 UOC samples randomly selected from the Canadian NNFL, representing 20 manufacturers from 8 distinct geographical locations and four types of UOCs, and
3. Three samples of unknown origin.

The origin of each sample was determined using classification models developed under the NMS/PAC and trained using the Canadian NNFL. To assess the effects of measurement specific uncertainty, the models were trained on different subsets of elements. The element subsets were chosen based on:

1. Prior measurements and geochemical subject matter expertise (published in (2));
2. Identification of elements with high variability and low measurement uncertainty in the dataset; and
3. Inclusion of the full suite of rare earth elements into the high variability subset.

The subset of elements included during the model-training phase is found to be crucial for reliably successful UOC attribution. Method 2 provided the best results: the ranges of concentrations of the elements were sufficiently broad to allow for clear discrimination between producers. In addition, it appears that the uncertainties in element concentrations play a significant role. Classification based on elements with lower uncertainties provided higher confidence in provenance assessment. The inclusion of rare earth elements in the training subset resulted in a decrease in the confidence of attribution, as already reported (2).

The significance of these results for the characterization and provenance assessment of UOC and interrogation of NNFL will be discussed.

References


State
Canada

Gender
Male

Primary authors: Dr JOVANOVIC, Slobodan (Directorate of Environmental and Radiation Protection and Assessment, Canadian Nuclear Safety Commission); Dr KELL, Tara (Directorate of Environmental and Radiation Protection and Assessment, Canadian Nuclear Safety Commission); Dr EL HADDAD, Josette (Energy, Mining and Environment Research Centre, National Research Council Canada); COCHRANE, Chris (Canadian Nuclear Safety Commission); Dr EL-JABY, Ali (Directorate of Security and Safeguards, Canadian Nuclear Safety Commission, Government of Canada)

Presenters: Dr JOVANOVIC, Slobodan (Directorate of Environmental and Radiation Protection and Assessment, Canadian Nuclear Safety Commission); Dr EL-JABY, Ali (Directorate of Security and Safeguards, Canadian Nuclear Safety Commission, Government of Canada)

Track Classification: MORC: Nuclear forensics
Building Sustainability into National Nuclear Security Regimes

The fundamental underpinning of nuclear security is a State’s national nuclear security regime, consisting of the legislative and regulatory framework, responsible institutions and organizations, and nuclear security systems and measures. To be truly successful, the nuclear security regime must be sustainable – reliably effective both now and in the future. The recently published IAEA Implementing Guide Sustaining a Nuclear Security Regime provides useful guidance on this topic. The paper complements this guidance by offering suggestions on how to build sustainability into the nuclear security regime – sustainability by design.

The fundamental goal is to create a nuclear security regime that institutionalizes nuclear security within the government of the State, competent authorities, licensees and other operating organizations, and civil society, so that nuclear security becomes self-sustaining. The paper describes several building blocks for this approach, including the following:

1. Establishing effective nuclear security as an enduring, apolitical, consensus-based norm – so that the nuclear security regime receives a consistently high level of attention and support, regardless of changes in leadership within the government, competent authorities, or operating organizations;
2. Embedding nuclear security in the permanent organization of the government – so that nuclear security is vested and weighted as a vital interest both within competent authorities for which nuclear security is a primary mission (such as the regulatory body) and within the sub-units of competent authorities for which nuclear security is one among many missions (such as law enforcement);
3. Appointing regulatory body leadership (such as governing board or commission chairs and members) to fixed multi-year terms – so that they gain an understanding of nuclear security and its importance and provide stability and continuity;
4. Developing nuclear security champions within the senior staff of regulatory bodies and other competent authorities, including designated successors with defined succession plans, so that nuclear security becomes a continuous high priority and does not suffer lapses when senior staff depart;
5. Professionalizing nuclear security through the establishment of degree and certification programs and the development of qualification requirements for licensees and other operating organizations – so that nuclear security specialists perform to well-defined levels of competency and nuclear security becomes an attractive long-term career path for talented individuals; and
6. Cultivating an appreciation of nuclear security fundamentals in professional societies and trade associations of related fields (such as health physics) – so that those of their members with nuclear security roles (such as radiation protection officers) take nuclear security seriously and are motivated and equipped to perform these roles well.

The paper describes these building blocks and several others in more detail. It then offers a template for assessing the extent to which they are in place in a given State, according to defined metrics, with suggestions for putting these items in place where they are absent or not fully developed.

State

United States

Gender
Female

**Primary author:** MANION, Jill

**Co-authors:** MORRIS, Frederic (Pacific Northwest National Laboratory); HAZEL, Michael (Pacific Northwest National Laboratory (US Department of Energy))

**Presenter:** MORRIS, Frederic (Pacific Northwest National Laboratory)

**Track Classification:** CC: Use of IAEA and other international guidelines for building national nuclear security regimes
This paper will discuss the need for devices to capture Industrial Control System (ICS) communication-based data within the architecture of a Nuclear Power Plant (NPP) in order to detect, investigate, or mitigate cyber-events. Furthermore, this paper will discuss requirements and design principles for such a mechanism.

Communication flows within NPPs are based upon security zones implementing the requirements of security levels. The five security levels within the IAEA’s example implementation in the Nuclear Security Series Draft on Computer Security Techniques for Nuclear Facilities (NST047) are described to cover, based on a graded approach to addressing the consequences of compromise, protection systems (Security Level 1), operational control systems (Security Level 2), supervision real time systems (Security Level 3), technical data management systems (Security Level 4) and other systems (Security Level 5).

In this regard, typically Security Levels 1, 2 and 3 form the ICS part of a nuclear power plant (Operational Technology - “OT”), while Security Levels 4 and 5 form the business portion of a NPP facility (Information Technology - “IT”).

This architecture contains various devices to record different sets of data for different purposes. A Process Historian collects information about the underlying physical processes and makes them available for operators. Usually this Process Historian is situated on a zone within Security Level 3. This historian must store the data for some given amount of time. A Plant Historian stores the information about the underlying physical process for the whole duration of a power plant’s operation. This data mostly serves analysts and system engineers. Such a Plant Historian resides on a zone underneath Security Level 4 and needs to be able to store data for a prolonged amount of time while ensuring the integrity of the data.

The business portion of the facility architecture often resides within a Security Information and Event Management (SIEM). The SIEM is tasked with collecting data about the IT processes within the zones comprising Security Level 4 and 5, as well as storing and analyzing this data. Data collected here is not so much concerned with the physical process, but instead “IT-Data”. Examples include the various properties of network communications or the state of the attached computing units. This data is relevant to detect potential security breaches.

As can be seen, there is currently no device responsible for capturing “IT-Data” within the OT-part of a plant’s architecture. However, the “IT-Data” available in this part of the overall architecture might prove helpful to identify, investigate, or mitigate security breaches. These data might include:
- information about network packets (to identify Flooding, Replay, Spoofing or Man-in-the-Middle attacks)
- information about the state of the processing units (to identify unusual cycle times within the processing units)
- aggregated information about this data in the form of events generated by anomaly detection systems situated within zones on Security Level 2 or 3

In addition, ICS protocol-specific information might be available (“ICS-Data”). This ICS-Data can also be correlated with the IT-Data and events. A device responsible for capturing this kind of data for the zones on Security Level 1–3 would require a mechanism to ensure integrity and authenticity of the collected data since an attacker might be interested in falsifying or destroying this data.

This paper will discuss the benefits of including an OT-SOC (Operational Technology Security Operation Center) and the usage of anomaly detection systems situated on zones within Security
Level 2 or 3 to act as probes for a modified SIEM (referred to as the Nuclear SIEM) on a Security Level 4 zone. This convergence of IT-OT data within a NPP architecture provides a holistic view of a plant’s data communications and provides a more advanced defensive posture against potential cyber-capable adversaries.


State

Germany

Gender

Not Specified

Primary authors: ALTSCHAFFEL, Robert (Otto-von-Guericke Universität Magdeburg); HOLCZER, Tamás (BME Crysys); NEAL, Christopher; HILDEBRANDT, Mario (Otto-von-Guericke-University of Magdeburg)

Presenters: ALTSCHAFFEL, Robert (Otto-von-Guericke Universität Magdeburg); HILDEBRANDT, Mario (Otto-von-Guericke-University of Magdeburg)

Track Classification: CC: Information and computer security considerations for nuclear security
Nuclear Power Plant in a Box

This paper presents the development of an architecture to deploy a simulated nuclear power plant in order to support training and research within the scope of CRP J02008. This simulated nuclear power plant ASHERAH consists of components covering the underlying physical process, the Industrial Control System (“ICS”) components supervising and controlling these processes and the IT components required to the associated business processes.

This architecture is created to be a. easily deployable, b. extendable, c. realistic in the simulation of the underlying physical process d. realistic in the behavior of its digital assets, e. allows access to a broad range of data and f. customizable for the use in training scenarios.

The Purdue enterprise reference architecture describes the structure of ICSs and the associated business systems in five different levels and three different zones according to their function. Within the Cell/Area-Zone, ICS functions are performed, while the Enterprise zone describes functions of classical IT-environments. Further information on NPP ICS architecture is defined by the IAEA’s example implementation in the Nuclear Security Series Draft on Computer Security Techniques for Nuclear Facilities (NST047). This implementation defines communication flows between various Security Levels and Security Zones. The five security levels within are described to cover, based on a graded approach to addressing the consequences of compromise, protection systems (Security Level 1), operational control systems (Security Level 2), supervision real time systems (Security Level 3), technical data management systems (Security Level 4) and other systems (Security Level 5).

These Security Levels roughly corresponds to the Purdue levels. Security Level 1-3 roughly aligns to the Cell/Area-Zone while Security Levels 4 and 5 align with the Enterprise Zone.

In order to create a realistic environment for training and research, the proposed architecture follows this hierarchy.

On the lowest level, a complex simulation of the physical processes is performed in order to supply the respective ICS with realistic input and enable realistic communication behavior between computing units, the attached sensors and the (simulated) actors. This simulation is performed using a MATLAB Simulink model.

Information about the simulated physical process is then passed on, using ICS communication protocols to the specific PLCs situated on Security Level 1-3 (or the Cell/Area-Zone). Currently, OPC UA and Modbus-TCP are employed to facilitate this communication. These physical input is then used to operate the given PLCs in a Hardware-in-the-Loop (“HIL”) fashion. In this area, realistic subsystem setups are used, using various PLCs and local HMIs which communicate using realistic ICS specific communication protocols. The structure of the underlying MATLAB model allows the usage of real physical sensors and actors instead of the simulated ones during testing.

The Enterprise Zone is implemented by virtual machines configured by Ansible to automatically deploy a broad range of various enterprise services. Some examples of the services on Security Level 5 are the internal and external email system, intranet and Internet access, web servers with proxies and network services (e.g. NTP, DNS, DHCP). On the Security Level 4 we implemented more specific services like work order management, change control management and plant historian services.

The overall architecture contains information flows from Security Level 1-3 to Security Level 4-5. Local HMI on Security Level 2 receive information from Security Level 1 components. A control Room HMI on Security Level 3 gather the information from the various Security Level 2 system. A Process Historian on Security Level 3 and a Plant Historian on Security Level 4 make this data available for further analysis.
The proposed architecture allows for the use in training scenarios, as it allows easy deployment, replication and the inclusion of various attack scenarios. The scope of the proposed architecture allows for complex cyber attacks spanning various attack steps as well as localized attacks employing single devices within subsystems. The architecture allows for the collection of data for the purpose of training, test and potential investigation.


Supply Chain Attacks Analysis based on opensource data

Recently supply chain attacks are becoming a number-one threat in cyber-security. Even for those companies who invest a lot of resources into building secured processes, physical security, cyber-security etc, supply chain attacks are one one of the weakest spots. Kaspersky Lab ICS CERT made a research based only on open source information that shows potential attack vectors on the supply chain for Nuclear Power Sector. This research contains analysis of the OSINT (Open Source INTelligence) methodology, analysis of Nuclear Power Sector service providers (supply chain), analysis of possible software and hardware used in Nuclear Power Sector and possible vulnerabilities, analysis of possible attack vectors and consequences of exploitation.

State
Russian Federation

Gender

Primary author: Mr DASHCHENKO, Vladimir
Presenter: Mr DASHCHENKO, Vladimir

Track Classification: PP: Nuclear security vulnerability assessments
Self-assessment of Nuclear Security Culture of Radioactive Source Users in BATAN: Survey and Interview

A self-assessment on nuclear security culture of radioactive source users have been conducted by CSCA in Pasar Jumat Nuclear Area, Indonesia, following a trial assessment that was conducted on Februari 2018. There are 5 (five) centers in the area with activities that are mainly using radioactive sources. This activity is based on the BATAN Chairman Directive Letter on April 2018 and currently two methods was performed, namely survey and interview. The CSCA deployed a survey team with 17 members to survey 353 employees. Meanwhile, the interviewer were 12 persons to interview 60 employees. These team members are experienced and well-trained on each method. The survey statements were developed in reference to a model of radioactive source security culture (CRPJO2007). A number of characteristics were selected from management system group, leadership behaviour group and personnel behaviour group within the model. The survey results were analyzed and categorized as follows: statements with highest score, statements with lowest score, and statements that are contradictory. There were also a number of written comments from survey respondents. Some survey results includes: different personnel behaviours in different centers, management system are not well implemented, and different behaviour between management level and staff level. Following the survey, positive hypotheses from highest score statements and negative hypotheses from lowest score statements were then developed. Subsequently, negative hypotheses were used as interview topics within the interview guideline, while positive hypotheses will be assessed by document review method. Some findings from the interview stage includes lack of security SOPs and lack of interaction or team work in problem solving. It is recommended that these findings need to be examine further by document review and observation methods.

State

Indonesia

Gender

Male

Primary author: Mr PURNOMO, Bayu (BATAN)

Co-author: KHAIRUL, Khairul (National Nuclear Energy Agency)

Presenter: Mr PURNOMO, Bayu (BATAN)

Track Classification: CC: Nuclear security culture in practice with a focus on sustainability
Integrated Training – Partnerships in Protection of Radioactive Materials

Protecting facilities that house high activity radioactive materials can be a challenge for any organization. The Office of Radiological Security (ORS) seeks to mitigate this challenge by providing physical security equipment and training assistance to sites who volunteer to participate in their program. Over the last ten years, the ORS Alarm Response Training (ART) has conducted over 180 training course for more than 6,400 participants from 48 U.S. states and 19 countries. Our ten years of success is due to the character of the ORS program. That is, never be complacent and always accept the challenge of contributing to improvement and being supportive of the participant’s needs. The program seeks to establish mutual, collaborative relationships on multiple levels and across non-traditional partnering organizations.

Establishing this integrated response course as it is today required several iterations before finding the right message. During this time, Alarm Response Training has captured hundreds of lesson learned and best practices while maintaining a continuous improvement process. Listening to the participants and partners and implementing changes where needed, we have helped the participating sites improve their security culture, develop response plans, and establish relationships among the Radiation Safety Officer/Health Physicist, on-site security, and the local law enforcement community. We have assisted teams of stakeholders, each with different personalities and divergent priorities, develop robust integrated plans to respond to a security alarm. Dealing with such a diverse audience of personnel required the message of the training be clear, meaningful, logical, and valuable to the participant.

With the aforementioned in mind, we applied a tutorial-type training program using subject matter experts with the same background as the attendees to convey the partnership and a “what’s in it for me” message. Engagement through a variety of traditional, performance, and sensory-based training has helped us achieve our goals. This method can be applied to facilities around the world in their efforts to better protect their radiological materials. This paper and presentation will discuss the teaching methods of ART, its evolution, and how we are preparing for the next phase of building partnerships through integrated training through new tools such as augmented reality and other sensory engaging methods.

State
United States

Gender
Male

Primary author: Mr WILLIAMS, Jimmie (US DOE)
Presenter: Mr WILLIAMS, Jimmie (US DOE)

Track Classification: CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for new
Low Energy Electron Beam as a Gateway to Machine Sources of Irradiation to Reduce Reliance on Isotope-Based Radiation Technologies

While Cobalt-60 and Cesium-137 have typically been used to irradiate materials for both research and industrial sterilization, the Office of Radiological Security (ORS) and its partners are investigating the viability of electron beam for various applications to reduce this radio isotopic footprint and improve global radiological security. Advantages of electron beam irradiation include lower capital costs than isotope-based technologies, the ability to turn on and off the machined source, the ability to deliver highly customized doses for specific applications, and the possibility of harnessing various e-beam energies for different applications. Currently, electron beam systems greater than 1 MeV require customized shielding and capital expenditure greater than $1 million for turnkey systems. Low energy e-beam systems (80 keV – 300 keV) allow for shelf-shielding and the possibility of in-line use in industrial processing. Today, low energy e-beam systems are in commercial use for polymer crosslinking, grafting, curing of printing inks, sterilization of aseptic food packaging, surface disinfection of eggs and seeds, and spice disinfection, etc. Greater availability of low energy e-beam technologies will catalyze research and development in the adoption of low-energy e-beam technology. Increased familiarity with low-energy e-beam technology can lead to greater interest and possible adoption of medium (1 MeV – 5 MeV) and high energy (7 MeV – 10 MeV) e-beam technology. There is an expanding interest in polymer modifications and other surface treatment processes in many regions of the world especially in the emerging markets in Latin America and Asia. Low energy e-beam technology is ideally suited for these applications. Presently, government programs provide cesium-137 irradiation users a financial incentive to switch to x-ray technology. The underlying hypothesis is that easy access to low energy electron beam technology by researchers can stimulate research and development programs in emerging countries in electron beam technology that in turn, can accelerate the transition away from cobalt-60 or cesium-137 technologies. This transition to machined sources such as electron beam will ultimately facilitate reduction of the risk while still maintaining current and in some enhances enhanced irradiation capabilities.

State

  United States

Gender

  Female

Primary authors:  ELSTER, Jennifer (PNNL); PILLAI, Suresh (National Center for Electron Beam Research)

Presenter:  ELSTER, Jennifer (PNNL)

Track Classification:  CC: Innovative technologies to reduce nuclear security risks and im-
prove cost effectiveness, where feasible
Adapting to Response - Customized Alarm Response Training

Monday, 10 February 2020 12:00 (15 minutes)

The Office of Radiological Security Alarm Response Training (ART) program provides a unique, quality training experience for sites participating in the voluntary security program. The training course is designed to cultivate interoperability of various response elements and offer the opportunity to discuss, develop, and refine their organizations’ response plans and strategies. The three day ORS ART course is held at the Y-12 National Security Complex in Oak Ridge, TN provides the participating site approximately ten slots. The ten slots are divided among on-site security, radiation safety, and local law enforcement personnel to ensure each response agency directly involved is represented. This “diversity of group” is essential in fostering an atmosphere of collaboration and is an element that consistently receives positive feedback in course critiques. However, because each site participating at the Y-12 site is limited to approximately ten slots, the majority of an area’s response personnel, particularly the law enforcement officers most likely to respond, are not afforded the opportunity of attending the training. Often, key leaders (e.g., police chiefs, city managers, and facility administrators) are unable to attend due to the schedule challenges presented by a weeklong training event held away from their jurisdiction.

Out of this request, the Customized Alarm Response Training Course (cART) was developed. The cART efforts complement, not supplant, the resident Y-12 program as the course often provides the first opportunity for participating sites to create and exercise tactics, techniques, and procedures (TTP’s). cART is strategically conducted in select cities across the U.S. In addition to providing on-site training, the cost for attending the cART is less than the current resident ART course since logistical support for approximately 40 participants is not required.

The cART program also provides the Local Law Enforcement Agency (LLEA) with a mock irradiator and supporting equipment. An example of equipment required includes a mobile camera system to provide central alarm station setups, observer rooms, and the ability to conduct after-action participant reviews.

The ORS program has implemented cART in through 2020 Cities Initiative. The 2020 Cities Initiative focuses on securing the top 20 cities by the year 2020. This paper will present the best practices and lessons learned from these select eve

State
United States

Gender
Male

Primary author: Mr WILLIAMS, Jimmie (US DOE)
Presenter: Mr WILLIAMS, Jimmie (US DOE)
Session Classification: Physical protection systems: evaluation and assessment
Track Classification: PP: Physical protection systems: evaluation and assessment
Advanced Malware and Nuclear Power: Past, Present, and Future

Cybersecurity in nuclear power is difficult to manage, overall. It is expensive to implement, regardless of the regulatory regime a plant is under. Technical controls are challenging to profile in many cases, as digital failure modes can be both difficult to model and can have wider ranging consequences than typical physical failures. Furthermore, intrusion detection and prevention controls for industrial systems can be much more expensive to deploy, as well as purchase or build. As a result, insight into likely future attack approaches, goals, and techniques will be invaluable in guiding future cybersecurity investment.

In the first section of this paper, we will examine noteworthy malware campaigns released over the past decade. We will identify key trends and areas of technical and procedural convergence between individual strains. We will examine current techniques, tactics, and procedures from both operational and technical perspectives. In the second section, we will conduct the same analysis over advanced malware strains that deliberately target industrial control systems. This will include older threats like Stuxnet and Flamer, as well as new threats like Hatman and CrashOverride. Both sections will focus on the adoption of new techniques and practices of malware attack teams rather than attribution. The main thrust of these two sections is to clearly outline the evolution of today’s general malware threats to establish a baseline of malware technical and procedural trending that we can compare and contrast with similar trends in advanced industrial malware strains.

Once we have been able to outline these evolving trends, highlighting both similarities and key differences between strains that target industrial systems and more general purpose strains, we will begin to hypothesize why those similarities and differences exist. For example, common initial infection vectors are radically different between advanced industrial and general purpose malware strains. Industrial strains typically rely on insider placement, while general families can take advantage of semi-commercial exploit kits. They both leverage phishing and spear-phishing approaches. In the case of industrial strains however, the phishing campaigns are much more targeted and deliberate.

We will then identify key trends in industrial malware capabilities and outline the impact of these trends on nuclear power plants, their operators, and industrial system manufacturers.

Over the past 10 years, we have seen a remarkable change in malware sophistication and the adoption of new strategies by malware authors. These kinds of approaches are beginning to appear in industrial malware strains as well. Although there are clear similarities in how malware is developed and deployed when comparing general purpose and industrial malware strains, there are distinct differences as well that are beginning to emerge. Both these differences and similarities have profound implications for nuclear power plant protection.

State
United States

Gender
Male
Primary author: LAMB, Christopher (Sandia National Laboratories)

Presenter: LAMB, Christopher (Sandia National Laboratories)

Track Classification: CC: Information and computer security considerations for nuclear security
Capacity-Building to Achieve Sustainable Security: Successful International Cooperation in the Dominican Republic

The U.S. Department of Energy/National Nuclear Security Administration’s Office of Radiological Security (ORS) cooperates with partner countries throughout the world to enhance the security of radioactive sources used for legitimate purposes. The IAEA and member states recognize that sustainability and capacity-building with partners is the foundation for a successful security program. There are a myriad of factors that can impede sustainability and capacity-building; nevertheless, a number of partner countries have enjoyed significant success in moving toward long-term security training initiatives and security culture development. The Dominican Republic is one country that has embraced its radiological security mission and taken remarkable strides toward establishing a sustainable radiological security structure. In addition to its development and enactment of the regulatory structure necessary to underpin its security efforts, the National Energy Commission (CNE) has been proactive in ensuring operators, regulatory staff, and response stakeholders in the country possess the tools and capabilities to properly implement their respective security responsibilities at fixed sites and have begun expanding these efforts to sources in transport. CNE not only convenes workshops to direct and assist operators in the development of site security plans, it also collaborates closely with law enforcement entities to develop and deliver training to response personnel to improve the effectiveness of a law enforcement response to an attempted theft of radioactive materials, and has convened stakeholders from across the response spectrum to maximize efficiencies and eliminate confusion during a multi-agency response effort resulting from the loss of control of radiological material. CNE recently evolved to a greater level of capacity building through its development of a curriculum for targeted training sessions to raise awareness of the threats, risks, and consequences associated with radiological or nuclear material; explain security management and related performance expectations; teach principles of security and security system design through hands-on instruction using physical security equipment in the training environment; ensure stakeholder awareness of the security requirements codified in national regulations; and emphasize security culture development among operators.

The example of the Dominican Republic offers several lessons that can be applied by other countries seeking to achieve similar success in capacity-building efforts. Analysis of the underlying conditions that have lent themselves to success in the Dominican Republic also helps identify areas where efforts can be focused to foster an environment where capacity-building can be more fruitful and sustainable security truly achievable. This paper will review the actions undertaken in the Dominican Republic, identify the circumstances that facilitated success and the hurdles overcome in the process, and seek lessons and best practices that can be applied in similar efforts elsewhere.

State
United States

Gender
Female
Primary authors: Ms MANION, Jill; ALMONTE DE HERNANDEZ, Narkiss Guzman (yes)

Co-authors: HAZEL, Michael (Pacific Northwest National Laboratory (US Department of Energy)); Mr TEJEDA, Olvir (Comision Nacional de Energia de la Republica Dominicana)

Presenters: Ms MANION, Jill; Mr TEJEDA, Olvir (Comision Nacional de Energia de la Republica Dominicana)

Track Classification: CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
Nuclear Forensics Signatures of Irradiated Fuel

The international community recognizes that an essential component of a national nuclear forensics capability is the development of a national nuclear forensics library (NNFL). The Canadian Nuclear Laboratories (CNL, formerly Atomic Energy of Canada Ltd.) is contributing towards the development of Canada’s NNFL. Given its unique expertise and access to data, CNL is conducting research into identifying potential forensics signatures of irradiated nuclear fuels used in pressurized heavy-water reactors (PHWR).

As part of the Canadian nuclear industry’s fuel development program, testing of experimental and prototypical fuels has been on-going for decades. This program of fuel testing and performance assessments, including predictive reactor physics code calculations, fuel characterization, and post-irradiation examination (PIE), has accumulated a considerable amount of information on fuels of different types, including uranium and mixed-oxide fuels. The objective of the current research is to determine potential forensics signatures of irradiated PHWR fuels based on isotopic ratios and fission product content. This paper presents correlations of isotopic composition of irradiated fuels obtained from code calculations, validated with actual measured data obtained from PIE.

State

Canada

Gender

Male

Primary author: Dr DIMAYUGA, Francisco (Canadian Nuclear Laboratories)

Co-authors: Mr BARRY, Aaron (Canadian Nuclear Laboratories); Mr CORBETT, Stavros (Canadian Nuclear Laboratories); Mr EDWARDS, Geoffrey (Canadian Nuclear Laboratories)

Presenter: Dr DIMAYUGA, Francisco (Canadian Nuclear Laboratories)

Track Classification: MORC: Nuclear forensics
Anomaly detection for network traffic of I&C systems based on neural network

Monday, 10 February 2020 11:30 (15 minutes)

With the increasing application of digital technologies in I&C systems, traditional protection strategy that depends on physical isolation is not enough. The I&C system is a type of cyber physical system, so it faces cyber security problems. Difficulties of cyber security in I&C systems are in three aspects. First, because I&C systems connect with process devices, cyber security of I&C systems requires high real-time performance. Second, I&C systems need to operate continuously, so prevention or detection approaches in I&C systems must minimize their impacts on operating I&C systems. The third one is that the consequences of cyber-attacks on I&C systems may be serious. It may not only influence the I&C systems but can also damage the nuclear reactor. Therefore, the cyber security strategies of I&C systems should be high real-time, careful and effective.

Anomaly detection for network traffic of I&C systems based on neural network is discussed in this paper. An anomaly detection software runs with the I&C systems. Network traffic data is extracted from mirror port in operating I&C systems, in form of network packets. This way of extracting data has little impact on the system. If anomalies are detected by the software, it will send alarm to the I&C systems so that responses will be implemented. Because the anomaly detection software works in real time, the anomaly detection approach only utilizes historical data and current data. The anomaly detection approach is based on neural network. Historical network traffic data of I&C systems are collected for training a neural network. The network packets are arranged in time order. Features are extracted based on only one current packet or both current and historical packets. The features are input into the neural network for training. Then the trained neural network is applied in the anomaly detection software.

The performance of software is test in an industrial control system testbed first. A neural network is trained using network traffic data captured from the testbed, and a software is established. However, the amount of data in the testbed is much less than that in operating I&C systems. In the next phase, several critical ports are chosen as mirrored ports in I&C systems. And the accuracy of the software is test using the data captured from I&C systems. At the same time, with the amount of data increasing, the structure of the neural network might be more complicated or combination of more than one neural network is needed.

State

China

Gender

Female

Primary authors: SI, Wen (Institute of Nuclear and New Energy Technology, Tsinghua University); LI, Jianghai (Institute of Nuclear and New Energy Technology, Tsinghua University); HUANG, Xiaojin (Institute of Nuclear and New Energy Technology, Tsinghua University); Ms ZHANG, Fan (Uni-
Anomaly detection for network tr...

Presenter: SI, Wen (Institute of Nuclear and New Energy Technology, Tsinghua University)

Session Classification: IAEA Coordinated Research Programmes for Information and Computer Security

Track Classification: CC: Information and computer security considerations for nuclear security
Breaking Siemens Protocol and Cheating on Distributed Control Systems

With the effort of industrial control system vendors, industrial network protocols are getting hardened and seems secure for last several years. Based on secured industrial network protocols, most of control system have getting updated. Especially, Siemens products widely used in industrial control system have well-made protection and security. However, the number of threats against Siemens products has been increased by cyber criminals. They have been working on vulnerability hunting on these products so that they could targeting most advanced facilities as many as they want.

Siemens s7comm Plus protocol presented with improvements on security such as against replay attack. A few cyber security researchers already analyzed this latest protocol then announced there might be another threat still existed. In this cyber security field like irresistible force paradox, vendors are always trying to update the security flaw. In 2019, however, this well-crafted and secured protocol’s mechanism is figured out in final. Its weak point could be used for logic tampering, man in the middle and replay attack between human-machine interface and Siemens S7-1500 programmable logic controller which is latest version.

The purpose of this paper is to inform how this well-made protocol could be analyzed and how it could affect to industrial control system. To conduct experiment for proving the research, physical condenser system was built as part of coordinated research projects. With this set-up, Siemens s7comm plus has been analyzed and tested security flaws that affect to other industrial control system in the same network zone. This paper will give an overview of how it’s possible to tamper memory of programmable logic controller and deface screen of human-machine interface with newly founded vulnerability of s7comm plus, and eventually turned to deceive all systems communicating in the same network. As like this, several feasible attack scenarios caused by this vulnerability and each step from the beginning of analysis to deceiving distributed control systems in nuclear power plants.

To abridge technical part, present research is done with vulnerability of s7comm plus protocol and frame a hypothesis how it affects TIA portal which is a software to develop control system and WinCC advanced which is human-machine interface from Siemens and other control system. The encryption mechanism of s7comm plus has been analyzed with debuggers and custom script codes. Main dynamic-link library of encryption algorithm to secure network traffic of s7comm plus has been figured out as well as specific functions in program. Only left part of this research is writing attack code with this vulnerability then deploy to any industrial control system to compromise it in the same network area.

State
Republic of Korea

Gender
Male

Primary authors:  Mr LEE, Seungjun (NSHC Inc.);  Mr MOON, Heaeun (NSHC Inc.);  Ms KIM,
Youngsun (NSHC Inc.)

**Presenters:**  Mr LEE, Seungjun (NSHC Inc.);  Mr MOON, Heaeun (NSHC Inc.);  Ms KIM, Youngsun (NSHC Inc.)

**Track Classification:** CC: Information and computer security considerations for nuclear security
An overview of Vietnam’s research activities on emerging technologies for Nuclear Security in the digital age: current opportunities, future outlook and the IAEA support

The list and the fields of emerging technologies in the digital age may have endless applications, but it can be categorized into several major workforces, such as the Internet of Things (IoT), big data, machine learning (ML)/ artificial intelligence (AI), encryption and communication technologies. Undergone more than 10 years in the development of nuclear security regime, Vietnam is one of the Member States which actively collaborated with the IAEA and other countries to equip the technology in the field of nuclear security. Entered in the fourth generation of the industrial revolution, like many other developing countries, Vietnam has faced a number of opportunities and challenges in sustaining and strengthening the national nuclear security regimes. In the last few years, Vietnam has conducted several research projects and international collaboration program in the subject of new science and technology for nuclear security concerns, especially the IAEA Coordinated Research Project (CRP) code J02005, entitled: “improved assessment of initial alarms from radiation detection instruments” and the CRP code J02012, entitled: “advancing radiation detection equipment for detecting nuclear and other radioactive out of material out of regulatory control”. This paper presents an overview picture of Vietnam on-going research and development activities on emerging technology in the digital age for nuclear security concerns, including: joint efforts to the IAEA and other partner countries in building big data for border detection, machine learning for support the front line officer’s decision making, communication technologies for radiation detection equipment and physical protection system, potential blockchain for the national integrated nuclear security network. The existing infrastructure, opportunities and desired future developments will be shared and discussed. A primary objective of this paper is to foster for using science and technology to sustain and strengthen the nuclear security regime in Vietnam as well as the other Member States, with the IAEA coordination and assistance.

State
Viet Nam

Gender
Male

Primary authors: NGUYEN, Ninh Giang (Vietnam Agency for Radiation and Nuclear Safety); Mr PHAN, Huu Phat (Ba Ria Vung Tau Customs Department)

Presenter: NGUYEN, Ninh Giang (Vietnam Agency for Radiation and Nuclear Safety)

Track Classification: CC: Advances in nuclear security research and development; international cooperation on nuclear security research
Development of the 435-B Type B(U) Package for International Disused Sealed Radioactive Source Recoveries

Without proper end of life management, disused sealed radioactive sources (DSRSs) become increasingly vulnerable to loss, theft, and sabotage that can result in accidents and incidents, including loss of life. Type B quantities of radioactive material can be particularly hard to manage due to complexity and costs associated with their compliant shipment from user's facilities to sites for final disposition or secure long-term storage. Historically, a major part of this issue stems from the lack of certified Type B packaging for safe, secure, and legally compliant shipments.

To help address this issue, in 2009 the U.S. Department of Energy (DOE), National Nuclear Security Administration (NNSA) Office of Radiological Security (ORS) directed Los Alamos National Laboratory (LANL) to design, test, certify, and fabricate Type B packages for domestic and international use. Through these efforts, the NNSA Model 435-B Type B (USA/9355/B(U)-96) was developed. The package was certified by the U.S. Nuclear Regulatory Commission (NRC) in 2014. Since then, three 435-B packages have been fabricated. Two are currently in use by ORS's Off-Site Source Recovery Program (OSRP) for DSRS recovery and disposal operations. In 2019, the third unit was donated to the International Atomic Energy Agency (IAEA) by the U.S. DOE/NNSA for international source recovery missions.

The 435-B package can be shipped by ground, air, or water. The relatively compact and light design (2245 kg empty weight) allow it to be used in locations with less developed infrastructure, such as unpaved roads. This was achieved by relying on payload shielding rather than adding significant shielding to the package itself, which would result in a very heavy, cumbersome Type B container. Shielded Type B containers can weigh upwards of 30,000 kg. Because the 435-B is unshielded, proposed payloads are thoroughly evaluated for their shielding properties and intrinsic safety prior to NRC certification as approved content. The list of approved 435-B payload content continues to grow as needs are identified.

As a part of the original conceptual design of the 435-B package, ORS and LANL anticipated that some international DSRS recoveries would be coordinated with the IAEA. To facilitate this, final design requirements included certification of the long-term storage shield (LTSS) as authorized content in the 435-B package. The LTSS is a lead-shielded container in which high activity DSRSs can be loaded using the IAEA mobile hot cell.

State

United States

Gender

Primary authors: WALD-HOPKINS, Mark; COEL-ROBACK, Rebecca (Los Alamos National Laboratory); TAPLIN, Temeka (Department of Energy- NNSA)
Presenters: WALD-HOPKINS, Mark; COEL-ROBACK, Rebecca (Los Alamos National Laboratory); TA-PLIN, Temeka (Department of Energy- NNSA)

Track Classification: PP: Transport of nuclear and other radioactive material: practices, challenges and regulatory issues
High performance gamma ray spectroscopy as a precision tool for nuclear forensics

For many decades, gamma ray spectrometry has been a key technology employed by laboratories for the identification of radioactive materials. Through this method, the detection of specific radioactivity can be indicative of nuclear events (ranging from nearby nuclear incidents to distant nuclear tests detected in global monitoring networks) or the process history and origin of nuclear materials and by-products. Over the past decade, there have been dramatic advancements in this method, where state-of-the-art laboratory systems are now combining multiple detectors and exploiting various technologies to be able to detect the smallest amounts of radioactivity. Additionally, this evolution allows for the unambiguous identification of the nature of the nuclear event or origin of nuclear materials and by-products, providing crucial information in support of nuclear security.

This work presents an international effort to evaluate the performance of gamma ray spectrometers for the support of these nuclear forensic applications. Carefully selected environmental samples, measured by various radiation laboratories across a multitude of detector technologies, serve as a benchmarking exercise to illustrate the radiation detection capabilities of these systems. Participants include Canadian laboratories at Health Canada and SNOLAB, international partners such as the Atomic Weapons Establishment in the United Kingdom, among others. At the forefront of this field, the multi-detector systems along with those located in deep-underground laboratories are pushing the limits of this method and advancing multiple domains, including: inspections for illicit nuclear materials, nuclear explosion monitoring, nuclear safeguards, and nuclear non-proliferation monitoring.

State
Canada

Gender

Primary authors:  Dr MEKARSKI, Pawel (Radiation Protection Bureau, Health Canada); Dr UNGAR, Kurt (Radiation Protection Bureau, Health Canada); HOFFMAN, Ian (Health Canada)

Presenter:  Dr MEKARSKI, Pawel (Radiation Protection Bureau, Health Canada)

Track Classification:  MORC: Nuclear forensics
The Application of a Systems-Based Approach to Computer Security at Nuclear Facilities

Many member states have chosen to adopt the use of compliance-based approaches when addressing the computer security of nuclear facilities. Such approaches typically mandate the application of a large set of generic security controls to protect every declared sensitive (i.e. critical) digital asset within a facility. The resulting volume of work has resulted in a significant challenge for some nuclear facility operators and competent authorities with respect to implementation and inspection activities.

Although there is merit in a compliance-based approach, it is important to be aware of potential drawbacks. One concern is that under a compliance-based approach, computer security engineers may need to spend a disproportionate amount of time preparing engineering justifications for why specific security controls cannot (or should not) be applied within the nuclear operational environment rather than working to secure sensitive systems from cyber threat. Another concern is the lack of a graded approach to the protection of sensitive systems related to safety, security, and emergency preparedness. If no grading criteria exists with respect to the relative importance of the system to the facility, then everything must be considered equally critical. This can result in applying the same time and resources to securing assets whose compromise poses little risk to the facility and those whose compromise poses much greater risk. There is also the concern that the compliance-based approach may lead to an asset-based mindset. This could result in a situation where the computer security analysis focuses so heavily on impacts to individual assets, it may fail to appropriately consider potential impacts to the design-based functions of the system that can arise when multiple assets are negatively affected by a given cyberattack.

An alternative or supplement to a compliance-based approach involves the use of a phased, systems-based approach that focuses on the protection of design base functions of sensitive systems. With this type of approach, systems are evaluated to (1) determine their relative level of susceptibility to compromise along identified pathways of communication and (2) the consequences resulting from a successful cyberattack. A risk-informed analysis in the systems-based approach provides the technical basis for the selection of security controls to mitigate consequences of cyberattacks.

This paper will report on some of the issues nuclear facilities and competent authorities have experienced with the compliance-based approach for computer security. The paper will identify where the appropriate application of a systems-based approach, as a supplement to (or modification of) the traditional compliance-based approach could improve computer security at nuclear facilities.

State

United States

Gender

Primary authors: LANDINE, Guy (Pacific Northwest National Laboratory); GLANTZ, Clifford (Pacific Northwest National Laboratory)
Presenters: LANDINE, Guy (Pacific Northwest National Laboratory); GLANTZ, Clifford (Pacific Northwest National Laboratory)

Track Classification: CC: Information and computer security considerations for nuclear security
Utilizing Reactive Model Systems to Elucidate the Chemical Context of Undeclared Radioactive Contaminants: A Case Study of the Ruthenium-106 Contaminant Detected in Europe 2017

Compositional and structural analysis to reveal the chemical context of interdicted nuclear or radiological material is a fixture of nuclear forensics, as regulated material originating from the nuclear fuel cycle will possess characteristic signatures that reveal its processing history and origin. In the limiting case, atmospheric detection of ultra-trace levels of radioactive material may play surrogate to lawful interdiction. In this instance, the virtual absence of stable material precludes the use of traditional forms of physiochemical analysis. How then do we access information pertaining to the chemical context of the radioactive contaminant?

Such was the case in October 2017 across Europe, with the detection of ruthenium-106. Using this instance as an example, we describe, for the first time, the use of selected reaction systems to reveal key information about the chemical composition of the ruthenium-106 contaminant. With systematic variation of reaction conditions, and examination of the subsequent fate of the ruthenium-106 contaminant, both general and highly specific deductions can be made to this effect. This information constitutes valuable empirical evidence to support a greater international investigative effort on the nature and origin of this material.

State

Canada

Gender

Primary authors:  Dr COOKE, Michael (Radiation Protection Bureau, Health Canada);  Dr HOFF-MAN, Ian (Health Canada);  Dr UNGAR, Kurt (Radiation Protection Bureau, Health Canada)

Presenter:  Dr COOKE, Michael (Radiation Protection Bureau, Health Canada)

Track Classification:  MORC: Nuclear forensics
A New Approach to Insider Threat Mitigation: Lessons Learned from Counterintelligence Theory

According to the International Atomic Energy Agency’s (IAEA) Information Circular (INFCIRC) 908, because “insiders possess access...authority and knowledge...[they] pose an elevated threat to nuclear security.” Insiders, witting or unwitting, working together or alone, possess the opportunity to cause significant damage to nuclear facilities through sabotage or unauthorized removal of nuclear or radiological material. In response to this global threat, INFCIRC/908 pledged nearly 30 countries, with assistance from the IAEA and INTERPOL, to establish and implement a range of national-level measures to better mitigate insider threats at nuclear facilities. However, the relative lack of publicly available insider case studies involving nuclear facilities makes causal analysis and pattern recognition—which are necessary to better devise and propose effective protection/mitigation efforts—difficult. Some insider threat researchers and practitioners have leveraged lessons from other disciplines to address this challenge. Prominent contributions to insider threat analysis include studies of high value jewelry heists and analyses of security measures within the casino and pharmaceutical industries.

One untapped discipline with key conceptual and practical similarities for eliciting insider threat mitigation insights is the field of counterintelligence. Counterintelligence, defined by United States Executive Order 12333 as “information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations,” provides a useful corollary to insider threat. Both counterintelligence and insider threat mitigation seek to protect high-value (or sensitive) assets from malicious, intentional human actions. Each discipline must contend with the challenge of identifying perpetrators from individuals with access rights that give them a privileged position compared to a traditional ‘outsider’ threat. In addition, the high security atmosphere of the Intelligence Community more closely approximates the uniquely protected environment of a nuclear facility than other civilian industries. Lastly, the consequences of failed counterintelligence and insider threat mitigation activities can both result in grave damage to national security.

This paper summarizes lessons learned from comparing conceptual similarities and empirical trends between counterintelligence activities and insider threat mitigation at nuclear facilities. After briefly reviewing insider threat lessons learned from other industries, this paper introduces the fundamentals of contemporary U.S. counterintelligence practice, including background investigations, mandatory reporting requirements, and the use of anomaly indicators for investigative purposes. Next, the paper outlines a comparison rubric and analytical framework for evaluating program goals, perpetrator characteristics, and protection efforts between counterintelligence and insider threat mitigation. Using U.S.-based counterintelligence case studies from the past several decades, this paper identifies key trends and insights across the motivations, characteristics, actions, and investigations applicable to insider threat mitigation. Lastly, this paper provides conclusions and lessons for potentially improving insider threat programs at nuclear facilities.


State

United States

Gender
Primary authors: WILLIAMS, Adam (Sandia National Laboratories); Mrs CAMP, Noelle (Sandia National Laboratories)

Presenter: WILLIAMS, Adam (Sandia National Laboratories)

Track Classification: PP: Insider threats
Preparedness and Implementation of Nuclear Security Plan for MPEs in Viet Nam

Nuclear security for major public events (MPEs), such as a sporting event or a high-level political meeting is very important for each country, and the organization of these events presents unique security challenges, including possible threats involving nuclear or other radioactive material. Understanding these challenges, Viet Nam requested support from the International Atomic Energy Agency (IAEA) to prepare and implement Nuclear Security Plans for several MPEs.

With the support from the IAEA, Viet Nam have implemented security plans for Hung King Temple Festival in 2016, APEC Summit in 2017 in Da Nang, and North Korea–United States (US) Summit in Hanoi in 2019. In order to execute these Security Plans, we developed Nuclear Security for MPE Architecture including the participation of various ministries and agencies under management of the Prime Minister, and a Joint Action Plan for the MPEs was developed between Viet Nam and the IAEA.

In order to organize the events we have planned Nuclear security response preparedness, such as organization of coordination meetings with experts from the IAEA and the US to discuss threat assessment, international assistance and nuclear security arrangements. Workshops, training courses, and technical visits to study and exchange experience on nuclear security for MPEs were conducted. During these training courses and workshops, we developed nuclear security scenarios and carried out exercises to enhance prevention, detection and response capability and to test the coordination among agencies involved. In preparation for MPEs, radiation detection instruments were installed, acceptance testing performed, detection and response procedures developed and tested, and pre-event radiological surveys and background mapping conducted.

Through the implementation of nuclear security plans for the MPEs, we recognize that it is important to have the involvement of the Government, the Ministry of Public Security and relevant Ministries; the valuable support of the IAEA and the US on providing experts, equipment, methods, and materials, and the great effort of the relevant organizations; and comprehensive preparedness.

We also found that security for MPEs needs comprehensive planning, systematic preparation and effective implementation of the nuclear security plan at the MPE.

We believe that conducting such nuclear security activities is an important step in improving the capacity of and providing experience for organizations and individuals involved in planning and implementing nuclear security measures at other major public events in the future.

State

Viet Nam

Gender

Female

Primary author:  Ms THAN, Thi Ngoc Mai (Viet Nam Agency for Radiation and Nuclear Safety)
**Co-author:** Mr NGUYEN, Tuan Khai (Viet Nam Agency for Radiation and Nuclear Safety)

**Presenter:** Ms THAN, Thi Ngoc Mai (Viet Nam Agency for Radiation and Nuclear Safety)

**Track Classification:** MORC: Nuclear security as part of the security of major public events
Lessons Learned from Developing the Graduate Nuclear Security Curriculum at the Kyiv Polytechnic Institute

As nuclear fuel cycle activities grow and the amount nuclear material increases worldwide, there will be a similar increasing need to more deeply incorporate nuclear security knowledge, skills, and abilities into nuclear energy workforces across the globe. To address this need, the International Atomic Energy Agency (IAEA) has provided NSS No. 12—Education Programme in Nuclear Security—as a technical guidance document and has created the International Nuclear Security Education Network (INSEN) to facilitate development and implementation of such programs. While both this best international guidance and voluntary engagement network establish a strong foundation for creating an educational capability in nuclear security, each individual nation is responsible for crafting such programs that both meet their specific needs and align with their national educational systems.

In response, the Ministry of Energy and Coal Industry of Ukraine has partnered with the U.S. National Nuclear Security Administration’s International Nuclear Security (NNSA/INS) program to develop a graduate curriculum in nuclear security at the National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute” (KPI). The main criterion of the choice of KPI is the availability of a laboratory base in Kyiv (in the center named after George Kuzmich) and the research reactor BVV-M at the Institute of Nuclear Research of the National Academy of Sciences of Ukraine, which can be used to prepare students. The Ukrainian government also agreed with this approach. Over the past several years, KPI professors have interacted with subject matter experts in multiple nuclear security-related topic areas from both NNSA/INS and Sandia National Laboratories (Sandia) to discuss how to build, implement, and maintain a nuclear security education program. These discussions have leveraged both IAEA-based guidance, Sandia expertise, and KPI’s education mandate to identify and develop courses in nuclear security-related topics to help meet the needs of Ukraine’s nuclear energy sector. With the support of their various governmental stakeholders, the KPI professors have diligently and effectively crafted a nuclear security curriculum that meets academic requirements across a variety of traditional disciplines, including engineering, physics, chemistry, and political science. Officially launched in the Fall semester of 2019, the KPI graduate program in nuclear security will provide a sustained source of human capacity development and education to meet national and regional nuclear security needs.

This paper will first review the history of collaboration between KPI and NNSA/INS and introduce how these engagements helped shape the progression of the curriculum and the professional development of the program’s professors. Next, the structure and description of KPI’s nuclear security program will be described, including a summary description of each course and how the learning objectives of each course correspond to the overall goals of the program. Lastly, the paper will provide several lessons learned—from both development process and from the initial implementation stages of KPI’s curriculum—to inform (and, hopefully) assist other nations embarking on developing nuclear security education programs.


State

Ukraine
Gender

**Primary authors:** Dr BIBIK, Tymofii (National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"); WILLIAMS, Adam (Sandia National Laboratories)

**Presenter:** Dr BIBIK, Tymofii (National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute")

**Track Classification:** CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
The Application of Maturity Models for Evaluating Computer Security Programs at Nuclear and Radiological Facilities

Maturity models, like the Cybersecurity Capability Maturity Model (C2M2), are applicable for nuclear and radiological facilities. The C2M2 was developed by the U.S. Department of Energy to allow critical infrastructure organizations to evaluate the general capabilities of their computer security programs in a consistent manner, communicate capability levels in meaningful terms, prioritize computer security investments for targeted areas of concern, and track how the maturity of their computer security program is changing over time. The C2M2 is designed for use by any critical infrastructure organization—regardless of ownership, structure, or size. Broad use of the C2M2 and the sharing of C2M2 results enables organizations in the United States to benchmark their performance. The C2M2 and similar maturity models are designed to be quick and easy to use. It can take as little as an hour or as much as a few days to complete a C2M2 analysis—with the amount of time dependent on the size and complexity of an organization/facility and its computer security program. The C2M2, or similar computer security maturity models, can help decision makers at nuclear and radiological facilities understand the status of their computer security program, set goals for the future, and make risk-informed decisions on how to achieve their computer security goals.

The C2M2 or similar maturity models may be used at multiple levels within a nuclear or radiological facility. For example, C2M2 results may be used operationally by:

- Decision makers who control the allocation of resources and are responsible for the management of security risks for the entire organization (not just its nuclear and radiological facilities)
- Managers responsible for a nuclear or radiological facility’s operations, safety, and security
- Security, computer security, and information technology professionals at a nuclear or radiological facility
- Staff members responsible for conducting computer security self-evaluations at a facility.

The C2M2 is built on a foundation of existing computer security standards, frameworks, programs, and initiatives. The model features 10 security domains; examples of which include Identity and Access Management, Threat and Vulnerability Management, Supply Chain and External Dependencies Management, and Workforce Management. Performance in each security domain is characterized using a structured set of practices. The practices represent activities an organization can perform to improve computer security in their domain. For example, the Workforce Management domain is composed of practices that an organization can perform to establish and enhance its workforce’s computer security capabilities. Sample practices include:

- Computer security responsibilities are assigned to specific people.
- Security vetting is performed at an organization-defined frequency for personnel with access to key digital assets.
- Computer security training is provided as a prerequisite to granting access to digital assets.
- Computer security awareness activities are conducted to reinforce training.

The C2M2 defines four maturity indicator levels, 0 through 3, which apply independently to each domain in the model. To earn a maturity level in a given domain, an organization must perform all of the practices for that maturity level and its predecessor level(s). For example, an organization must fully or largely achieve all the practices prescribed for maturity level 1 and 2 to achieve an overall maturity level of 2 in that security domain.

Striving to achieve the highest maturity level in all domains may not be the optimal business solution. For example, a small facility that manufactures radiopharmaceuticals may be able to overcome the consequences of a successful cyberattack better than a nuclear facility (as the competent authority may shut down the nuclear facility for weeks or months longer than the radiopharma-
ceutical facility owing to the greater safety and security risk (and stakeholder interest) associated with an incident at a nuclear facility. In such a case, the computer security maturity level that is the goal of the organization operating the radiopharmaceutical facility may be somewhat less than the goal for the nuclear facility.

A given organization or facility might value performance in some security domains more than others. The C2M2 provides flexibility for an organization to target different maturity levels for its security domains based upon its defined business objectives. The benefits and costs of computer security programmatic activities should be evaluated against the risks and costs of a successful cyberattack when selecting appropriate goals for a nuclear or radiological facility’s computer security maturity levels. This paper will report on the application of computer security maturity models for nuclear and radiological facilities and illustrate how these models can be used to guide planning for computer security programs.

State

United States

Gender

Primary author: GLANTZ, Clifford (Pacific Northwest National Laboratory)

Co-authors: SKARE, Paul (Pacific Northwest National Laboratory); LANDINE, Guy (Pacific Northwest National Laboratory); GOURISETTI, Sri Nikhil Gupta (Pacific Northwest National Laboratory); MYLREA, Michael (Pacific Northwest National Laboratory)

Presenter: GLANTZ, Clifford (Pacific Northwest National Laboratory)

Track Classification: CC: Information and computer security considerations for nuclear security
Preliminary Results from Invoking Artificial Neural Networks to Measure Insider Threat Mitigation

Insider threat mitigation programs have traditionally focused on preventative and protective measures to mitigate insider threats (and resulting malicious acts) to nuclear facilities. Preventive measures—including pre-employment background investigations—are those implemented before trusted access is provided to nuclear facilities. Protective measures—including the two-person rule for accessing more sensitive facility locations—are those implemented after trusted access is provided. These approaches tend to focus on identifying and deterring the problematic or malevolent behaviors of individuals instead of evaluating collective behaviors observed in the facilities. This approach has resulted in an overreliance on generic job tasks analysis and detection of aberrant behavior that does not account for patterns of workplace behavior, ignores facility recovery operations, and lacks adequate measures of mitigation effectiveness.

In response, research from across the government and private sector has hypothesized ways to utilize empirical data from increasingly networked security and facility “health-monitoring” systems to improve, and even automate, portions of insider threat mitigation programs. More specifically, this research argues that a better understanding of workplace dynamics will improve the ability to identify, detect, and forecast the potential for a successful insider threat action. This type of approach better integrates workplace behavior-related insights into traditional insider threat mitigation programs. These advances, while important to the long-term success of insider threat mitigation programs, are based on differentiating between malicious intent and natural “organizational evolution” to explain observed anomalies in collective workplace dynamics, trends, and patterns.

To better understand how these patterns impact insider threat mitigation efforts, a collaborative research project between the U.S. National Nuclear Security Administration’s International Nuclear Security Program (NNSA/INS), Sandia National Laboratories (Sandia), and the University of Texas at Austin (UT-Austin) collected empirical data on work patterns at the Nuclear Engineering Teaching Laboratory (NETL)—a TRIGA MARK II research reactor facility—at UT-Austin. Signals collected from door access readers, video surveillance, area radiation monitors, and personnel radiation detection portals were combined with a commercially available software tool from ReconaSense to quantitatively describe insider threat potential and evaluate mitigation effectiveness. More specifically, this project leveraged the ability of artificial neural networks to synthesize—and learn from—disparate data sources (e.g., card access readers) for perform anomaly detection. This project also applied resilience algorithms to describe insider threat mitigations in terms of well-known theories of organizational behavior. This paper summarizes a new approach for understanding, identifying and evaluating insider threats—including a more advanced evaluation framework and set of measures—capable of improving related mitigation measures at nuclear facilities.


State
United States

Gender
Primary authors: WILLIAMS, Adam (Sandia National Laboratories); Dr CHARLTON, William (Nuclear Engineering Teaching Laboratory, University of Texas); Mrs ABBOTT, Shannon (Sandia National Laboratories); Mrs CAMP, Noelle (Sandia National Laboratories); Mr WALLACE, Eric (Sandia National Laboratories); Mr ROSS, Michael (Sandia National Laboratories); Dr TERRY, James (Nuclear Engineering Teaching Laboratory, University of Texas)

Presenter: WILLIAMS, Adam (Sandia National Laboratories)

Track Classification: PP: Insider threats
Exploring the Security/Safety (& Safeguards) Interface to Mitigate Risks in the Nuclear Fuel Cycle

Part of the challenges to the creation of responsible nuclear energy programs—including new, novel activities within the nuclear fuel cycle (NFC)—lies in evaluating safety, security, and safeguards (or, nonproliferation) mechanisms. While traditionally implemented and evaluated independently across NFC activities, recent calls from the global community suggest the need for an “all hazards” approach to developing responsible nuclear energy programs. Yet, such an “all hazards” approach necessarily includes a complex, dynamic, and interdependent set of risks and threats to the responsible implementation of NFC activities.

Recent complex systems engineering research has argued that properties such as security (and safety) emerge from interactions between technical, human, and organizational components within systems. For NFC activities specifically, these insights suggest a benefit from evaluating risk complexity across and between safety, safeguards, and security. Such an interdependent analytical framework would help identify gaps, interdependencies, conflicts, and leverage points across traditional safety, security, and safeguards approaches. A better understanding of these security/safety (and safeguards) interfaces could also better align analysis and design with real-world operational uncertainties and better describe the risk complexity associated with new, novel NFC activities.

In response, Sandia National Laboratories’ (Sandia) Mitigating International Nuclear Energy Risks (MINER) Program has explored the application of systems theory principles (e.g., emergent behaviors) and complex systems engineering concepts (e.g., multidomain interdependence) to better understand and address these risks and threats. Sandia’s MINER research perspective reframes the discussion around the risk complexity of NFC activities to address interdependencies between safety, safeguards, and security. This Sandia research explored the safety, safeguards, and security risks of three different nuclear sector-related activities—international spent nuclear fuel transportation, small modular reactors, and portable nuclear power reactors—to investigate the complex and dynamic risk related to an “all-hazards” approach. This paper summarizes the technically rigorous analysis of the safety, safeguards, and security risks of these three NFC activities and introduces a systems-theoretic approach for exploring interdependencies between the technical evaluations.

Evaluating these different NFC activities showed that a systems-theoretic approach can better identify interdependencies, conflicts, gaps and leverage points across traditional safety, security, and safeguards risk mitigation strategies than traditional approaches. This analytical perspective supports popular safety, security, and safeguards “by-design” proposals for NFC activities and has helped identify key implications for NFC activities at these interfaces. As a result, “all hazards”-based mitigation strategies from applying systems theoretic principles and complex systems engineering concepts can be (1) designed to better capture interdependencies at the security/safety (and safeguards) interfaces, (2) implemented to better align with real-world uncertainties, and (3) evaluated as a “systems-level” whole to better develop responsible nuclear energy programs. These conclusions and implications serve as waypoints for completing next steps toward advancing the technical understanding of safety, safeguards, and security for new, novel NFC activities.


State
Gender

**Primary authors:** WILLIAMS, Adam (Sandia National Laboratories); Dr OSBORN, Douglass (Sandia National Laboratories)

**Presenter:** WILLIAMS, Adam (Sandia National Laboratories)

**Track Classification:** CC: Nuclear safety and security interfaces
Building Capacity to Strengthen Nuclear Security: The path to a sustainable nuclear industry

Nuclear Security is a very important topic when it comes to the peaceful uses of nuclear energy. The history of the nuclear energy sector has concentrated its efforts in safeguards and safety, focusing on how to avoid proliferation and military uses of the nuclear technology, and how to protect the population and the environment from harmful effects of a possible radiation. However, as a milestone, the 2001 World Trade Center terrorist attack changed the way the world faces the terrorist threat, especially when it comes to the nuclear technology. The new reborn "pattern" of terrorism implies new adversaries, tactics, techniques and ways to attack. And now, the threat is global, leaving no place on earth away from this conflict. Adversaries are willing to do anything, by all means, everywhere, and not only specifically to Government or military facilities, but to the general population and "soft" and civilian targets.

With this new terrorism pattern, the nuclear technology could become an asset to spread fear, death and cause a huge psychological harm attached to a conventional explosive device. And the threat is real. For example, the IAEA ITDB and open source internet information has proven the willingness from different terrorist organizations to acquire this material to conduct malicious acts against society and the environment. That is why nuclear security is a growing topic among member states, and something that should develop nationally, but also regionally and as a global community.

That is why countries has to focus their efforts in building different capacities to strengthen nuclear security. This means, assess the needs for training and to conduct different capacitation to the technical personnel as well as law enforcement, on a diverse topics such as nuclear detections, emergency response, nuclear forensics, security during transportation of nuclear and radiological materials, insider threat mitigation, cybersecurity, among many others. A given country should further develop its capacities on nuclear security, upgrading and updating its protocols, procedures, equipment and knowledge on those topics. And then training and re-assessing its capabilities.

The protection and security of nuclear and radioactive materials becomes a top priority given the emergence of new threats. Building capacities on nuclear security, especially in countries with a middle range develop nuclear energy, helps acquire more social license, develop a more legitimate industry and guarantee a secure activity. This is the only way to achieve a sustainable nuclear industry.

State
Argentina

Gender
Male

Primary author: BIEDA, Tomas (Ministry of Energy and Mining)
Co-author: Mr DELUCHI, Facundo (Undersecretariat of Nuclear Energy)
**Presenter:** BIEDA, Tomas (Ministry of Energy and Mining)

**Track Classification:** CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
On the Application of Causal Inference to Incident Response in Nuclear Facilities

The digitalization of Instrumentation and Control (I&C) systems in nuclear facilities introduces the potential for cyber-attacks to result in operational effects on critical systems. There have been several high-profile incidents that have demonstrated this potential, including the Stuxnet virus in 2010, which targeted the nuclear sector, and the cyber-attacks to electrical distribution networks in the Ukraine in 2015. In these cases, and in others, a cyber-attack resulted in significant consequences for the physical process under control.

Threats of this type implement a so-called kill chain – a series of activities that an adversary must complete to achieve their goal – that can be realized over several months and involves the compromise of numerous computer systems. It is possible that such an attack will be blended with a physical compromise of a target facility, e.g., via an insider. An adversary will attempt to remain stealthy (undetectable) until the point the attack on the physical system is executed. Therefore, indicators that a facility has been compromised via a cyber-attack could be weak and not readily attributable to its observable consequences. Consequently, a cyber-attack may exhibit the characteristics of a fault or another non-malicious root cause. This can make the execution of appropriate and targeted computer security incident response activities difficult.

To help detect the effects of threats that target the physical domain, there are several approaches that aim to identify anomalous behaviour that is being exhibited by a process. In many cases, these approaches involve learning the normal behaviour of the process and detecting deviations from the learned norm. Abnormalities could be caused by a cyber-attack or other non-malicious challenges. To determine whether a detected anomaly has been caused by a cyber-attack (or otherwise), other systems that indicate the root cause of an anomaly can be used. For example, intrusion detection and anti-virus systems can be used to support a hypothesis that the root cause of a detected anomaly in a process behaviour is a cyber-attack.

For cyber security, combining this information is typically achieved by correlating indicators; however, this may yield misleading insights as correlated events are not necessarily causally related. An approach to addressing this issue is to use causal models – which can capture expert knowledge – that describe the relationships between indicators of anomalous behaviour and the likelihood they have a certain root cause. Using such models, an operator can infer the likely root cause, e.g., expressed in terms of a system state, associated with detected anomalous behaviour, and use these inferences to guide an incident response.

In this paper, we present a novel application of an approach to causal inference to support incident response in nuclear facilities. This approach builds on anomaly detection algorithms that aim to detect deviations from the normal operation of nuclear processes and systems within a facility. The aim is to indicate and evaluate the utility of using causal models to infer the root causes of anomalous behaviour to support computer security incident response. This is done using scenarios that have been developed in the IAEA Coordinated Research Project (CRP) J02008 on incident response in nuclear facilities. In the project, a hypothetical Nuclear Power Plant (NPP), called Asherah, has been developed, which includes a simulation model of a Pressurized Water Reactor (PWR). Experimental results using the Asherah simulator, which has been coupled with representative computer systems, indicate how causal models can be used to determine the root cause of anomalous behaviour. We comment on how this capability can expedite incident response activities in nuclear facilities.

REFERENCES


State

Austria

Gender

Primary authors: Dr PIATKOWSKA, Ewa (AIT Austrian Institute of Technology); Mr ALLISON, David (AIT Austrian Institute of Technology); SMITH, Paul (AIT Austrian Institute of Technology); HEWES, Mitchell (IAEA)

Presenters: Dr PIATKOWSKA, Ewa (AIT Austrian Institute of Technology); SMITH, Paul (AIT Austrian Institute of Technology)

Track Classification: CC: Information and computer security considerations for nuclear security
Improving National-Level Guidance to Local Nuclear Safety Programs

Our paper examines how local variations in policies, procedures, and regulations affect the value of national-level guidance and programs for local jurisdictions developing nuclear and radiological security capabilities. It also suggests a framework for additional research into these variations. Efficient prevention, detection, and management of radiological and nuclear threats requires the formal inclusion of local jurisdictions within a nation-state’s nuclear security framework. This tenet is well-established, with many examples of international and national guidance and programs featuring the important role of local jurisdictions in nuclear and radiological security, such as:

- Proceedings from The Safety of Radiation Sources and Security of Radioactive Materials—a 1998 conference organized by the IAEA, the European Commission, INTERPOL, and the World Customs Organization—address how local jurisdictions, especially local law enforcement agencies, help safeguard radiation sources both inside and outside of regulatory control, dating back more than 20 years.
- The United States Department of Homeland Security (DHS) offers a variety of technical assistance and funding programs that support local jurisdictions’ efforts to prevent, detect, and manage nuclear and radiological threats, including the Securing the Cities program, which offers grants to major cities to support nuclear detection architectures.
- The Japan Atomic Energy Agency’s (JAEA’s) Nuclear Emergency Assistance and Training Center (NEAT) provides training for national and local-level emergency responders and officials involved in nuclear emergency preparedness and response.

Although thoughtfully developed, current national guidance and programs for nuclear and radiological security (such as those above) tend to treat local jurisdictions uniformly. Within the United States, however, a closer examination of state and local nuclear and radiological prevention and detection programs reveals important variations in relevant policies, procedures, and regulations that affect how these jurisdictions execute their security operations. These variations lead to challenges that are not yet addressed by most national guidance or programs.

Through our work with more than 15 state and local nuclear and radiological security programs in the United States, we have identified more than 10 areas of variation across jurisdictions that can impact local operations, including the following two examples:

- Secondary screening for radiation sources outside of regulatory control: Local jurisdictions typically exercise broad authority to conduct primary screening, which may include radiation detectors placed in major transportation hubs or police officers carrying personal radiation detectors during special events. If a radiation detector is alerted, however, what actions are public safety officers authorized to take? What if members of the general public are not cooperative? State and local interpretation of relevant law varies significantly, creating inconsistency and ambiguity for secondary screening operations. Much national-level guidance in the United States either does not address this issue, or addresses it very generally.
- Transportation of radioactive materials: Although the U.S. Nuclear Regulatory Commission and the U.S. Department of Transportation are largely responsible for the control of radioactive material transport, states decide on when and how to provide escorts for many types of radioactive materials traveling on their highways. These varying procedures among states challenge the sharing of best practices and the utility of uniform national-level guidance.

Our initial research underscores how nationwide variability across local jurisdictions in the United States is affecting the effectiveness of existing national guidance and programs. We recommend applying a framework to comprehensively identify additional areas of variation. DHS created a taxonomy of 32 core capabilities to assist the realization of the U.S. National Preparedness Goal. While this taxonomy is intended to support the management of all-hazards—natural disaster, in-
tential threats, and technological accidents—it also provides a convenient organizing construct to understand how local jurisdictions pursue radiological and nuclear management differently and how their challenges vary. It has worked well to guide our research efforts.

Although based on observations made in the United States, our findings likely apply to other nation-states as well. Moreover, we assert that the core capability framework provides a generalizable means of structuring facilitated discussions and further research to identify variations with important ramifications. Ultimately, we believe that systematically applying this framework will help guide opportunities for national and international agencies to better support radiological and nuclear security operations in a more comprehensive yet customized manner.

State
United States

Gender
Female

Primary author: Ms MOHRES, Erin (CNA)
Presenter: Ms MOHRES, Erin (CNA)

Track Classification: CC: Emergency preparedness and response and nuclear security interfaces
Computer Security Training and Exercises in the Nuclear Sector: Insights from a User-centered Requirements Gathering Process

Computer security is recognized an important aspect of nuclear security, as highlighted by Resolution GC(62)/RES/7 of the IAEA 62nd General Conference (2018), which encourages States to take effective measures against cyber-attacks. An important measure – highlighted in the Resolution – is the provisioning of computer security training courses. The nuclear sector, with support from agencies such as the IAEA, is responding to the need for training and exercises. As the sector’s response matures, it is useful to understand and evaluate the current state-of-play, as perceived by the (potential) recipients of training. With this understanding, informed guidance about future strategic directions for training and exercises can be made, to ensure that initiatives provide the most benefit to participants and the sector.

The contribution of this paper is two-fold: first, we describe a campaign for gathering requirements for computer security awareness and training in the nuclear sector, which was conducted in the framework of the IAEA’s CRP J02008 (Enhancing Computer Security Incident Analysis at Nuclear Facilities). In this context, we share a set of challenges and recommendations for implementing user- and stakeholder-centered thinking in the given multi-stakeholder setting. We critically reflect approaches to implement an iterative consultation process and to embed diverse user involvement tools into this process, such as audience participation and personalized electronic questionnaires.

The second contribution is a survey of the status of computer security awareness and training within the nuclear sector, as yielded by the requirements gathering process. Participants from thirteen countries across different roles and organization types (e.g., operator, regulator, policy maker, contract support) engaged in an electronic questionnaire and personal interviews that aimed at identifying the perceived computer security risks, the current state of computer security education within their organizations, as well as impediments to education and key improvement measures for increased awareness and protection.

The results of our research show that safety system operation ranked highest among seven different areas of risk, and that ‘removable media and devices’ was the most strongly perceived attack vector. Participants outlined the most important impediments to increasing computer security awareness and skills in their respective organizations – namely, a lack of management focus and support, a lack of priority or applicability, and insufficient personnel to conduct the training. According to the respondents, the human factor is considered in nuclear computer security programs of their organizations, but education is often regarded limited. The current focus of computer security training in many facilities is on building awareness and development of skills, and less targeted at regulatory compliance, process validation or skills re-enforcement, which reflects the emerging nature of human-centered computer security in the nuclear sector. Findings of this nature motivate the need for continued engagement from the IAEA to support Member States in the development of nuclear sector-specific training, as proposed in Resolution GC(62)/RES/7.

The paper concludes with recommendations both for the design of requirements gathering processes and improved computer security training and exercises in the nuclear sector. To advance computer security education in this field, different approaches should be considered, according to their applicability for the individuals using them: For both theory-driven and hands-on computer security education, participants preferred scenario-based approaches, followed by game-based approaches for knowledge and awareness building, and by field exercises for practical application. Ranking key factors showed that industrial control system considerations and implementing computer security incident response plans should be addressed within the next larger training activities. A further aspect that became apparent is that awareness and knowledge building measures should...
be consistently evaluated, in a similar way as is already common for practical exercises.

The research leading to these results has received funding from the IAEA as part of the CRP J02008 on Enhancing Computer Security Incident Analysis at Nuclear Facilities.

State

Austria

Gender

Primary authors: Ms REISINGER, Michaela (AIT Austrian Institute of Technology); Dr FRÖHLICH, Peter (AIT Austrian Institute of Technology); SMITH, Paul (AIT Austrian Institute of Technology); HEWES, Mitchell (IAEA)

Presenters: Ms REISINGER, Michaela (AIT Austrian Institute of Technology); Dr FRÖHLICH, Peter (AIT Austrian Institute of Technology); SMITH, Paul (AIT Austrian Institute of Technology)

Track Classification: CC: Information and computer security considerations for nuclear security
Engaging Law Enforcement Responders to Ensure Effective Security for Radiological Materials

The U.S. Department of Energy/National Nuclear Security Administration’s Office of Radiological Security (ORS) cooperates with partner countries throughout the world to enhance the security of radioactive sources used for legitimate purposes. As codified in the IAEA’s Nuclear Security Series Number 11, Security of Radioactive Sources, effective radiological source security is based upon systems that can properly perform the key security functions of detection and assessment, delay, and response. Each of these security functions is dependent upon a human factor for successful execution, but the response function, which “encompasses the actions undertaken following detection to prevent an adversary from succeeding...” is based almost completely on personnel supported by equipment, rather than equipment supported by personnel.

In order to optimize the effectiveness of response to attempted unauthorized removal of radioactive material, response personnel must understand three key concepts: first, understanding the consequences associated with the malicious use of radiological or nuclear material in order to accord associated response activities an appropriate level of importance and prioritization; second, recognizing both the risks associated with ionizing material and the measures they can take to mitigate those risks in order to effectively interrupt an adversary without facing unnecessary personal risk; and third, understanding the realities of security systems that protect the target material in order to properly analyze the adversary timelines and take measures needed to ensure appropriate response times can be achieved.

One additional complication must also be overcome in order to ensure a reliable response function: engaging a critical mass of law enforcement personnel in order to be confident that responders who may be on-shift during a theft event have the proper training and awareness to respond effectively.

To address these challenges, ORS engages its partner country stakeholders through multiple training courses for law enforcement personnel to convey the key response concepts to a broad constituency. This strategy serves to address the need to expose a critical mass of law enforcement personnel to the necessary ideas, as well as initiate the growth of a security culture among law enforcement personnel that encompasses radiological material and develop appropriate advocates who will ultimately champion the adoption of this response training as part of a broader law enforcement training curriculum.

In Poland, ORS has experienced success with this approach to response engagement and training. As a component of the broader ORS Global Cesium Security Initiative (GCSI), ORS trainers undertook a regional approach to responder engagement. This broader and deeper approach resulted in a highly effective partnership with Polish response stakeholders. The joint cooperation has led to the cultivation of a broad cadre of trained response personnel. More importantly, Polish response stakeholders have led a successful effort to both adapt radiological theft response training to meet the country’s particular needs and to integrate the training curriculum into the existing training programs at police academies and training facilities in Poland. The partnership between Poland and ORS offers a number of lessons for response engagement initiatives to ensure investment of training resources in this area will bear fruit and achieve intended objectives.
Gender
Male

Primary author:  HAZEL, Michael (Pacific Northwest National Laboratory (US Department of Energy))
Co-authors:  Mr JAMISON, Jeremy (Pacific Northwest National Laboratory); MANION, Jill
Presenter:  HAZEL, Michael (Pacific Northwest National Laboratory (US Department of Energy))

Track Classification:  PP: Risk-informed approach to the security of radioactive material in use and in storage
Nuclear Security in CHILE: Benefit of INSSP Missions and others.

The responsibility of Nuclear Security in Chile is of the State and the Chilean Nuclear Energy Commission, among other organizations, has been working this topic in the country. In 2012, Chile received a mission of the International Atomic Energy Agency (IAEA), for the National Strengthening of Nuclear Security, which main objective was to conduct a diagnosis of the six functional areas of the Integrated Plan for Support of Nuclear Safety (INSSP). The following year, 2013, a mission of the International Nuclear Security Advisory Service (INSServ) missions was carried out, for the evaluation of the national architecture of nuclear and radiological safety, and its detection and response capabilities, with emphasis on border monitoring. In 2018, a new mission is carried out, this time to update the INSSP Plan, where most of the member organizations of the Commission on Safety and Security for Radiological Emergencies (CONSER, acronym in Spanish) participate. This Commission is a body created to advise and support the Presidency of the Republic, in the strengthening of the capacity of prevention and reaction of the competent institutions, for nuclear or radiological events which may affect the public safety, the integrity of the people or the environment. In the same way, the Department of Energy of the United States (DOE-US) has carried out cooperation and support missions, delivering training, courses and donations of detection equipment to organizations, which response for nuclear security events. Finally, the Global Initiative for the Combat of Nuclear Terrorism, GICNT, has contributed and financed two binational exercises, between Chile and Argentina, carried out in the neighboring country, contributing to improve the nuclear security too.

This work is intended to show improvement of nuclear security in CHILE, from different support, especially INSSP missions.

These IAEA missions and the support received by the DOE-US and GINCT, in addition to the organization called CONSER; they have made it possible to advance and improve in the nuclear security requirements in the country, especially in interagency coordination and the improvement of response capabilities, among other relevant aspects.

Our nation continues working jointly on the issues of Emergencies and Nuclear Security and expects to continue counting with this support, to encourage and improve Nuclear and Radiological Security, as part of the State’s role of safeguarding public security and protecting environment.
Integrated Nuclear Security Support Plan
A Proven Approach for Effective Computer Security Self-Assessments at Nuclear Facilities

A proven method for conducting cyber security self-assessments at nuclear power plants is now available for international use. This method was originally developed by Pacific Northwest National Laboratory (PNNL) under contract by the United States Nuclear Regulatory Commission (USNRC) for use by U.S. nuclear power plant licensees. The "Method", described in NUREG/CR-6847 "Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants", was originally a limited release document that was withheld from public disclosure. The USNRC rescinded the document’s classification and it is now publicly available. The Method provides a systematic, phased, and risk-informed approach to help decision makers and security specialists understand their relative cyber security posture. The Method goes into more detail on how to make risk-informed decisions using information obtained during the self-assessment guidance than does the IAEA's 2016 publication, Conducting Computer Security Assessments at Nuclear Facilities. However, the two approaches are compatible, with the Method fitting neatly into the framework provided by the IAEA’s assessment guidance.

While the focus of the Method concentrates on systems associated with safety, security and emergency preparedness, it can also be extended to other systems within a nuclear facility (e.g. operational control systems associated with secondary or balance-of-plant operation, traditional IT systems related to business functions). Completed assessments may be used to support or validate the selection of computer security controls to mitigate cyber threats as well as demonstrate compliance with regulations or statutes enacted by Competent Authorities.

The Method assesses the cyber security posture of key systems at a nuclear facility with a focus on the protection of design base functions. It considers both physical and digital elements of system vulnerabilities and the resulting potential consequences from exploitation. It is well-suited for addressing blended cyber-attacks. A semi-quantitative analytical approach is used in the evaluation of potential vulnerabilities, consequences, and risks. The Method’s risk assessment provides a technical basis for the selection of security controls to mitigate cyber-attacks.

The Method consists of six stages that fit within the steps outlined in IAEA assessment guidance. These stages are:
1. Examination of plant-wide cyber security practices. The team gathers information on the facility’s cyber security policies, procedures, and practices. Information is also gathered on resources that can play a role in the cyber security of critical systems.
2. Identification of Critical Systems and Critical Digital Assets (CDAs) to be assessed. Systems associated with safety, security and emergency preparedness are identified. These systems are analyzed to identify and understand the digital assets that perform the design base function of the system. An initial consequence analysis for each identified CDA is used to estimate the potential consequences to the system and facility from a successful cyber-attack.
3. Conduct tabletop reviews and validation testing of the CDAs and their connected digital assets. Conduct tabletop reviews with plant personnel responsible for the design, operation, and maintenance of the identified critical systems and CDAs. Validation involves physical inspections (walk-downs) and a configuration review of critical systems. Where appropriate, an option exists to conduct scanning of CDAs and connected digital assets.
4. Conduct assessments of susceptibility. Results from the tabletop reviews and validation testing are used to assess the susceptibility to cyber exploitation of each CDA. Pathway analysis is used to understand the various vectors of attack that may exist for the system. Both direct and indirect pathways of compromise are considered. The product of this stage is an estimate of the overall susceptibility level for each CDA.
5. Conduct risk assessment activities. The initial consequence analyses that was performed in Stage 2 is reassessed using the additional information gathered in Stages 3 and 4. These results

May 9, 2020
are used in conjunction with the results of susceptibility assessments to estimate the risks of cyber exploitation for each identified CDA.

6. Conduct risk management activities. Identify and characterize potential new security controls that could be implemented to enhance cyber security. A cost-benefit analysis is performed to identify those security controls that maximize effective protection and minimize risks to operation. Effective risk management options and recommendations are prepared for senior plant management approval and implementation.

The Method’s application at U.S. nuclear power plants has been very encouraging. The only nuclear plant in the U.S. that did not have any adverse finding during its initial NRC computer security inspection prepared for its NRC inspection through the diligent application of this self-assessment method and the implementation of the recommendations that came out of that self-assessment. Nuclear facilities around the world might find application of the Method extremely helpful for making cost-effective, risk-based decisions regarding computer security and for preparing them to pass computer security inspections by their competent authorities. This paper will summarize the Method and report on its successful application.

State
United States

Gender

Primary author: LANDINE, Guy (Pacific Northwest National Laboratory)

Co-authors: GLANTZ, Clifford (Pacific Northwest National Laboratory); COLES, Garill (Pacific Northwest National Laboratory)

Presenter: LANDINE, Guy (Pacific Northwest National Laboratory)

Track Classification: CC: Information and computer security considerations for nuclear security
Developing Computer Security Regulations for Radioactive Material and Associated Facilities

Radioactive material and associated facilities are vulnerable to cyber attack. Possible adversary scenarios include disabling or spoofing computer-based security systems to gain unauthorized access to radioactive material, to an associated facility, or to security-sensitive information; compromise of computer-based accounting and inventory systems to mask theft or diversion of radioactive material by insiders; and sabotage of computer-based safety or operational systems in order to cause the release of radiation. To counter such scenarios, many regulatory bodies are developing or considering the development of regulatory requirements for computer security, as recommended by current and forthcoming International Atomic Energy Agency (IAEA) guidance.

The paper presents a framework that regulatory bodies could use to undertake this process. The framework consists of a series of questions that the regulatory body could address in deciding whether and how to develop regulatory requirements for computer security, as well considerations that would go into addressing those questions. The questions addressed include:

1. whether the regulatory body has the legal authority to impose computer security requirements;
2. whether to impose computer security requirements as part of general security regulations or as separate requirements or by other means such as license conditions;
3. what other competent authorities may need to be involved in the development and implementation of computer security requirements;
4. whether to use a performance based, prescriptive or combined approach to computer security requirements;
5. the types of adversary scenarios that the computer security measures implemented by operators should address;
6. the types of computer security requirements that regulations might include;
7. whether to vary the requirements based on practices (e.g. teletherapy versus industrial irradiator) or keep them generally applicable to all practices; and
8. how the operator will be directed to document compliance with the resulting requirements, for example in the operator’s security plan or in a separate computer security plan.

The paper also provides example regulatory provisions for different regulatory approaches to computer security. The result is a tool that can be used by regulatory bodies directly, in bilateral or multilateral regulatory development workshops, and in training on this topic.

State

United States

Gender

Male

Primary author: MORRIS, Frederic (Pacific Northwest National Laboratory)

Co-authors: Ms WEISE, Rachel (Pacific Northwest National Laboratory); DONELLY, David (Pacific Northwest National Laboratory)
Presenter: MORRIS, Frederic (Pacific Northwest National Laboratory)

Track Classification: CC: National nuclear security regulations
Evaluating Software Defined Networking Solutions to Reduce the Digital Attack Surface of Nuclear Security Systems

Most nuclear security systems in place today were not designed to address the current threat environment. Systems that were originally intended to be stand alone are now interconnected. Devices that have a single purpose are built on multi-purpose platforms and use communication protocols that, while effective, have no ability to authenticate authorized versus unauthorized commands. These attributes provide an attacker significant ability to affect the system, pivot throughout the interconnected networks, and remain undetected if he or she can compromise a single node.

Software defined networking (SDN) has been used for years by information technology cloud service providers to quickly provision or remove servers or other systems to meet changing demand. The same concept has recently been applied to operational technology systems to enable very fast failover on critical systems that have stringent and deterministic (<5ms) transmit/receive times. Using software defined networking, the communication flows through a network are carefully engineered using preplanned routes and specific pathways. This networking approach makes it possible to achieve deterministic and extremely reliable message delivery, even when components fail.

The engineering approach for software defined networking has added numerous security benefits, including but not limited to: securing the networking control plane, eliminating network scanning and mapping, inhibiting Address Resolution Protocol (ARP) spoofing and host masquerading, eliminating unauthorized network pivoting, and enabling greater situational awareness on the network.

Software defined networking in operational technology environments is a relatively new concept. Early testing conducted in electrical power and other critical infrastructure, however, has proven it to be a very effective tool for building reliable networks and reducing the digital attack surface of the network. Researchers at the Pacific Northwest National Laboratory and Idaho National Laboratory are testing software defined networking technologies on a radiation portal monitor system and physical protection system to validate its effectiveness in these common nuclear security systems. In these tests, researchers establish a baseline using existing networking equipment, then replace and configure the existing networking equipment with software defined networking equipment. Once the software defined networking equipment is in place, the team reruns the same tests used in the baseline.

In this paper, we will explain the concept of software defined networking in greater depth and provide an overview of the tests conducted on nuclear security systems and the results achieved. We will also discuss the security benefits of software defined networking in the context of nuclear security systems and consider other nuclear security applications beyond those that have been tested.

State

United States

Gender
Primary author: CLEMENTS, Samuel (Pacific Northwest National Lab)

Co-author: NICKERSON, Charles (Idaho National Laboratory)

Presenter: CLEMENTS, Samuel (Pacific Northwest National Lab)

Track Classification: CC: Information and computer security considerations for nuclear security
Providing Guidance for Creating Information Security Continuous Monitoring Programs to Support Transitioning to Ongoing Authorizations in Nuclear Security Programs

Historically, compliance-oriented computer security programs were built with a 'set it and forget it' mentality when it came to security control implementation in computing environments. Typically, the security control implementation would be revisited on a set multi-year recurring basis (e.g. every three years) where the security program would reevaluate the effectiveness of the security controls, make necessary security changes for the current operating environment, and seek reaccreditation from the Authorizing Official. This compliance-based approach to computer security is no longer considered an effective means of managing the security of today’s computing environments. Compliance-based programs are not adequate to show current system risks and fail to help provide mitigations to combat modern threats.

Computer security standards bodies have encouraged security programs for years to move to ongoing authorizations that do not have a set date for reaccreditation. The continuous accreditation of the system relies on enhanced, near real-time information about the current security health given the organizations understanding of current threats coupled with current mitigations. Moving to an ongoing authorization strategy is dependent on the establishment of an Information Security Continuous Monitoring (ISCM) program. ISCM programs establish key metrics the organization monitors and provides information which helps govern the overall security health of the computing environment. They create threshold triggers which are set to ensure corrective actions are taken if the metric points move outside the desired threshold bounds. In some instances, the metrics provide information which help lead to quick response when real security incidents occur.

Incorporating an ISCM program helps move organizational computer security programs from sluggish, compliance-based programs to agile, risk-based programs that can quickly adjust to the ever-changing threats of today’s computing environments. Nuclear regimes can enhance their ability to identify new threats and maintain current mitigations by adopting an ISCM program. ISCM program effectiveness has been vetted through years of use by various industries and when used appropriately by nuclear regimes, it will increase the efficiency with which nuclear security programs operate and provide better security for the industry as a whole. The paper would provide guidance specific to nuclear regimes on how to implement an ISCM program including relevant key metrics to monitor nuclear security systems which includes monitoring and assessment frequencies. The paper will also advise how the information from the selected metrics can be used to make rapid risk-based security decisions and how to assess your ISCM program to ensure the organization continues to track the relevant data to properly respond to emerging threats.

State
United States

Gender
Primary author: CHRISTENSEN, Drew (Pacific Northwest National Laboratory)

Co-author: CRAMER, Steven (Pacific Northwest National Laboratory)

Presenter: CHRISTENSEN, Drew (Pacific Northwest National Laboratory)

Track Classification: CC: Information and computer security considerations for nuclear security
The internet, which for years has been viewed as a global online commons with standardized protocols but few regulations, is, according to some experts, starting to mirror the contentious political and commercial contours of the physical world.

A number of problems, including data breaches, privacy debates, cyber enabled attacks on critical infrastructure, government surveillance operations, theft of intellectual property, and manipulation of electoral processes, have contributed to a growing skepticism in many states that an open internet will naturally serve the best interests of users, communities, countries, and the global economy. In addition, the rapidly emerging and increasingly lucrative power of data has global superpowers eager to protect their informational sovereignty as an urgent matter of national security.

Recognizing some of the problems associated with an open internet, a number of States have begun making efforts to isolate their domestic internet for political, economic, or social reasons. This trend towards a more fractured internet, or “splinternet,” has courts and governments embarking on what some call a “legal arms race” to impose a maze of national or regional rules, often conflicting, in the digital realm.

There is a need to evaluate the possible security implications if the internet does indeed fracture into a number of smaller, nationally-administered internets organized along geopolitical boundaries. While the status quo is not without its own vulnerabilities, a new structure may present new or different threats to the physical protection systems and cyber security measures that currently protect nuclear facilities and material worldwide.

Considering a potential future “splinternet,” this paper will specifically assess how a fractured internet may affect the various nuclear security systems operating around the world. Specific questions could include:

• Will fractured monitoring of malware threats increase the severity of malware outbreaks?
• Could less comprehensive evaluation of vulnerabilities further erode trust in safety/security systems?
• Will it be more difficult to provide robust configuration management across unique application domains?
• What are the safety and security implications for industrial control systems (PLCs and similar) if they become less standardized?
• If the Internet fractures along national borders, will it lead to new protocols and architectures for large networks?
• Will it enable or hinder attribution of bad actors in the digital realm?

State

United States

Gender
Primary author: GERHRIG, Lindsey (Pacific Northwest National Laboratory)
Co-author: GOYCHAYEV, Rustam (Pacific Northwest National Laboratory)
Presenter: GERHRIG, Lindsey (Pacific Northwest National Laboratory)
Session Classification: Risks and benefits to nuclear security from innovations in other fields, including artificial intelligence and big data
Track Classification: CC: Information and computer security considerations for nuclear security
Developing the design of the national nuclear detection architecture for material out of regulatory control using roadmap model

The growing concern of the international community relating to the security of nuclear and radioactive material after September 11th, 2001 resulted in a strengthening, at world level, of the application of nuclear security measures through the adoption of new parameters and methodologies for the design and implementation of effective nuclear security detection architecture (NSDA). The risk of that nuclear material or other radioactive material be used in terrorist acts is considered a serious threat to international peace and security and cannot be overlooked in the current global situation. IAEA keeps a database of incidents and illicit traffic, containing confirmed reports on nuclear and radioactive materials detected out of regulatory control. These materials, a.k.a. MORC (Materials Out of Regulatory Control) may be used on criminal or terrorist acts. States have responded to this risk making a collective commitment to strengthen the security and control of this material in order to protect people, property, society and the environment from the harmful consequences of a nuclear security event. Therefore, State should design and develop a national NSDA to integrate nuclear security systems and measures needed to achieve goals of the national strategy for the detection of nuclear and other radioactive material out of regulatory control with sufficient and sustained resources for the various competent authorities to enable them to carry out their assigned functions, including establishing and maintaining systems and measures to detect, manage information assessment from instrument alarms, information alerts, qualitative and quantitative information concerning the alarm or alert, and information from other sources and initial assessment of the alarm or alert. Currently, Brazil doesn’t have a national strategy defined for the detection of nuclear and other radioactive material out of regulatory control, not having, for example, a minimal radiation detection capability at all points of entry, such as, seaports, airports and border crossings. This paper shows an efficient and visual tool, of easy understanding to develop a NSDA, based on the international recommendations, using the roadmap model, so as to make its adoption easier in Brazil. The challenge is even greater considering Brazilian territorial dimensions. Brazil has:

- Land borders with ten countries, totaling 16,885 kilometers with 36 formal international border crossings, representing the world’s third longest land border;
- Maritime border from north to south, totaling 7,367 kilometers with 44 seaports;
- 30 international airports.

It becomes important to promote, in the scope of the Brazilian nuclear security regime, a greater awareness on this matter, making it possible, specifically: to provide for the security of nuclear and other radioactive material and associated facilities and activities; to ensure the security of such material in use, storage or in transport; to combat illicit trafficking and the inadvertent movement of such material; and to be prepared to respond to a nuclear security event. Considering the national context regarding the country’s borders dimensions, stakeholder involvement and legal support in force, this work concludes that Brazil needs urgently to develop a NSDA based on a national strategy with well-defined scope and goals, to better follow the current world situation of radiological threats, and the best practices adopted internationally.
Gender

Male

Primary authors: ROZA DE LIMA, Alexandre (Brazilian Nuclear Energy Commission); ALVES TAVARES, Renato Luiz (CNEN - Brazilian National Nuclear Energy Commission); Mr MONTEIRO FILHO, Josélio Silveira (CNEN - Brazilian National Nuclear Energy Commission); AUGUSTO DA SILVA, FRANCISCO CESAR (Institute of Radiation Protection and Dosimetry)

Presenter: ROZA DE LIMA, Alexandre (Brazilian Nuclear Energy Commission)

Track Classification: MORC: Building and maintaining nuclear security detection architecture
Cyber Resilient Hardware Controller

General-purpose computation has launched entire industries and improved the lives of billions around the globe. But the speed of commerce has pushed application of networked computing to so-called Operational Technology (OT) such as industrial control system (ICS), programmable logic controllers (PLC) and other embedded systems including the Internet of Things (IoT) without full understanding of its security ramifications. Even sensitive and safety-critical infrastructures like the nuclear industry now depend upon the ubiquitous employment of these networked computerized devices. What has become apparent is the potential for the misuse of these system, as evidenced in media reports on how cameras and digital video recorders (DVR) were used to launch the largest distributed denial of service (DDoS) attack to date. To put it more succinctly: general-purpose computers, software, and operating systems used for single purpose applications (e.g., a safety controller or video camera) have excess capabilities that are a growing target of cyber threat.

Software-based solutions are extremely flexible and offer over-the-Internet maintenance updates that greatly reduce cost, and the resulting economic incentives influenced society to digitize/automate everything possible, even our critical infrastructures. Unfortunately, the convenience of networking and the monoculture created by commodity hardware and software have made these systems the great Achilles’ heel of our modern world. The commodity hardware may be far more capable than what is required for the process at hand. This extra capacity is attractive to attackers, as we learned from the Mirai botnet. Commodity software’s excessive capabilities extend the attack surface of the systems without benefitting the application.

Reducing this attack surface is the primary objective of this paper. We describe the development and test of a prototype controller that can execute process logic with only hardware. The hardware-only nature of our solution prevents the controller (or any other device built on the same principle) from being repurposed via malware or other network borne cyber-attacks. We solve the cyber problem by removing the software. Our approach employs a Field Programmable Gate Array (FPGA) instead of the vulnerable Von Neumann architecture. We will discuss the novel features of our current prototype and our planned path forward to replace the FPGA with a custom 3D-printed circuit board. Ultimately, 3D printing of circuitry could significantly reduce the cost and cycle-time of the typical Application-Specific Integrated Circuit (ASIC) design process, putting this ability into the hands of each company’s process engineer. A prototype controller was developed and tested in 2018 as a demonstration of how a hardware-only controller can be considered as a viable replacement for a PLC, a video camera controller or other IoT device without using software, which significantly reduces the cyber-attack surface.

The apparent inflexibility of hardware-only solutions used to be the major drawback, but their immunity to internet-borne cyber-attack is becoming a major advantage. If this type of system were widely available today, designers could deploy new systems, confident that they could not be maliciously repurposed. FPGA-based hardware-only controllers require physical access to override or replace their physically-programmed functions. They will be provably (not just theoretically) unhackable without direct physical access. The physical access requirement means that system-wide changes cannot simply be rolled out to a national enterprise from a remote location. It is true that the cost of updating hardware-based systems is higher on a per-controller basis. However, most infrastructure systems are not supposed to change function or be updated for decades at a time. Arguably, the reason most security updates or patches are needed today can be traced to the vulnerabilities of software. Thus, many security updates will no longer be needed. For critical infrastructures, the security afforded by this inflexibility will be a major strength that outweighs the incremental cost incurred by the rare need for system updates.

This paper will be presented along with a physical (or video-based) demonstration of the prototype and thereby stimulate a discussion about the possible directions within this field of study that
might provide more cyber resilient systems for use within the nuclear industry.

State

United States

Gender

Primary author:  PEDERSON, Perry (Pacific Northwest National Laboratory)

Co-authors:  FINK, Glenn (Pacific Northwest National Laboratory);  CHRISTMAN, Nicholas (Pacific Northwest National Laboratory)

Presenter:  PEDERSON, Perry (Pacific Northwest National Laboratory)

Track Classification:  CC: Information and computer security considerations for nuclear security
Computer Security Training

Computers and the internet have changed our lives for the good in many ways, but with the change comes risk. In a nuclear regime, risk must be managed appropriately, and to do so, personnel must be properly trained.

1. INTRODUCTION
This paper explores the findings of the first-ever international training course (ITC) on Protecting Computer-Based Systems in Nuclear Security Regimes, and discusses dynamic ways of implementing a proper instructional strategy for a computer security training program. Computer security training must shift from a less academic feel to a facilitated approach with a more hands-on delivery technique that incorporates, stories, case studies, and scenarios.

Computer security has grown into a specialized field to help nuclear regimes stay secure. A good computer security training program has training that helps people apply what is taught. An appropriate instructional strategy aligns with a desired human performance after training has taken place.

2. APPROACH
The appropriate instructional strategy for entry level computer security training is a critical andragogical approach. Meaning, it has adult learners critically thinking about their current practices and helps them identify ways to implement better computer security techniques. This is done through case studies, scenarios, and stories that learners can relate to; that helps learners believe in the training. Once learners believe in the training, they will be more committed to their learning and will feel they need to know the principles taught. Then the likelihood of the learners implementing what is taught increases.

However, for more advanced skills a more hands-on approach is necessary using a situational cognition approach as the foundation of the instructional strategy. Meaning, learners get their hands-on equipment and apply some of the techniques taught within the training. The most critical part of situational cognition in a learning environment is to create a safe place for learners to experiment and learn from their mistakes.

During the first ever ITC on Protecting Computer-Based Systems in Nuclear Security Regimes, 97% of learners said they will implement principles they learned. It was also found, through the hands-on demonstrations and capstone at the end of the training, learners not only started to master higher level skills, but enjoyed the training and had significant interactions with other learners in the class. The following is the approach that was taken to create the ITC on Protecting Computer-Based Systems in Nuclear Security Regimes and implement the two instructional strategies discussed earlier in this paper.

- Identified a team of cyber security experts and an instructional designer
- Clearly defined the instructional strategies that aligned to adult learning behaviours
- Reduced PowerPoint and made a more cause and effect learning environment
- Created case-studies, stories, and scenarios
- Created life-like demonstrations with training equipment

3. CONCLUSION
With the appropriate instructional strategy optimal learning and improved human performance will take place. The ITC on Protecting Computer-Based Systems in Nuclear Security Regimes, is an example of effective training delivery to improve computer security.

State

United States
Gender

Primary author: PATRICK, Donald (Pacific Northwest National Laboratory)

Presenter: PATRICK, Donald (Pacific Northwest National Laboratory)

Track Classification: CC: Information and computer security considerations for nuclear security
Interim storage options for disused radioactive sealed sources to enhance end-of-life management

The Off-Site Source Recovery Program is a U.S. Government activity sponsored by the National Nuclear Security Administration Office of Radiological Security and managed at Los Alamos National Laboratory. The program mission is to remove, safely secure, and disposition excess, unwanted, or disused radioactive sealed sources that pose a potential risk to national security, public health, and safety.

The lack of access to immediate removal or permanent disposition pathways for disused radioactive sealed sources may pose a concern to source owners, regulatory authorities, and the public. During their useful service lives, radioactive sealed sources have numerous essential and beneficial uses in the fields of medicine, industry, construction, education, and research applications. However, due to their high activity and portability, some of these sources could be used, either individually or in aggregate, for malicious purposes resulting in economic impacts and significant social disruption. Examples of intentional misuse include radiological dispersal devices (RDDs), also called dirty bombs, and radiological exposure devices (REDs).

Once radioactive sealed sources become disused, the end-of-life management cycle begins. While safe and secure storage discussed herein is only a temporary measure, it is nonetheless an important step along the path between end-of-use and final disposition. A means for permanent disposition is essential but is unavailable in many cases. Therefore, secure interim storage may be necessary, potentially for an extended period of time.

In the absence of formal storage facilities, disused radioactive sealed sources may unfortunately be placed in closets, transportainers, sheds, basements, and other soft targets. Such unsecured storage locations pose a risk for both unintentional and intentional mishandling of sources. In some cases, the development of safe, easily constructible, and secure storage options at a minimal cost may be a viable option to prevent the loss or theft of disused radioactive sealed sources.

There are currently no adequate statistics on the number of disused radioactive sealed sources around the world, but the number may continue to rise due to increasing international deployment of radioactive sources in medical, agricultural, and industrial applications. Particularly in developing countries or remote areas, there may be a lack of formal secure storage facilities for disused radioactive sealed sources awaiting final disposition. It takes resources (time, funding, and personnel) for formal storage facilities to be conceived, designed, permitted, and constructed. In some regions, electricity for security systems may not be reliable or present at all. Therefore, it is suggested that considerations be made to utilize low-cost, secure, custom-built source storage options for use in a variety of areas and settings. In its simplest form, a small storage configuration could be constructed using readily available materials, personnel and equipment. It could also be provided as a kit to allow easy and inexpensive deployment, operation, and maintenance.

Because the ultimate end-of-life management goal for disused sources is permanent disposition, retrievability is an important consideration of interim storage. It is not uncommon for disused sources to be cemented into holes in the ground or other structures in such a way that subsequent recovery and disposal become difficult, if not impossible. With proper consideration, interim storage can be designed to allow for retrieval of disused sources while still providing substantial security against unauthorized intrusion.

In cases where expensive storage infrastructure is unrealistic, the benefit of employing this low-cost storage option outweighs the risk of doing nothing (e.g., unintended radioactive exposures or intentional misuse). While not meant as a final solution, safe and secure interim storage is still vital to permanent risk reduction by emphasizing a cradle-to-grave policy on disused radioactive sealed sources.
sources and bridging the gap between end-of-use and ultimate disposition of disused radioactive sealed sources.

**State**

United States

**Gender**

Not Specified

**Primary author:** GRIFFIN, Justin (Los Alamos National Laboratory)

**Co-authors:** Mr GURLEY, Michael (Los Alamos National Laboratory); COEL-ROBACK, Rebecca (Los Alamos National Laboratory)

**Presenter:** GRIFFIN, Justin (Los Alamos National Laboratory)

**Track Classification:** PP: Risk-informed approach to the security of radioactive material in use and in storage
Lost in Translation: Addressing Semantic Challenges in Nuclear Security Discourse across Languages

At international events on nuclear security, it is a near inevitability that, at some point, proceedings will grind to a halt as participants struggle to grasp or articulate the concept of "nuclear security" itself. This should pose little surprise: many languages - including four of the six official languages of the United Nations - use the same word to denote both "safety" and "security." After decades of International Atomic Energy Agency (IAEA) efforts to promote nuclear safety and, more recently, to bring security to a level on par with safety, the risk of confusion in this area remains rife. Unfortunately, the consequences of such confusion for perception, policy, and practice can be quite real, and have likely confounded efforts to promote nuclear security since their inception. To take an example, one of the most widely accepted and used official terms for "security" in Russian, физическая защита (fizicheskaia zashchita - physical protection), suggests a stark emphasis on outsider-adversary-oriented physical measures, rather than on areas such as culture, insider threat, policy and administration, and sustainability. And indeed, these different areas of emphasis tended to characterize U.S. and Russian efforts to cooperate directly on nuclear security, and their respective management of security in their own nuclear complexes. This paper will survey common translations and usages of the term "nuclear security" and key related concepts in several of the United Nations official languages (Russian, Chinese, and French) to identify pronounced semantic shortfalls and traps, and their potential consequences. The authors will then offer recommendations on how to address these, both in the initial choice of words in English and in translation. It is our hope that this work can serve as a reference for drafters, translators and interpreters, and can help augment the IAEA’s ongoing efforts to build an authoritative nuclear security glossary to facilitate the articulation and adoption of international nuclear security best practices.

State

United States

Gender

Male

Primary author: DONNELLY, David (Pacific Northwest National Laboratory)

Co-authors: KOVCHEGIN, Dmitry (Independent Consultant); RATZ, Leon (Nuclear Threat Initiative)

Presenter: DONNELLY, David (Pacific Northwest National Laboratory)

Track Classification: CC: Implementation of national legislative and regulatory frameworks, and international instruments
Enhancing the Sustainability of Nuclear Security in Newcomer Countries through Addressing Country-Specific Issues in Education and Training Programs

Newcomer countries introducing nuclear energy programs for the first time have the advantage of building on the vast experience accumulated by countries with already existing nuclear energy programs in the design, development and implementation of their nuclear security systems. On the other hand, newcomer countries face a number of challenges that, if not addressed properly, can strongly affect the sustainability of the nuclear security, which must exist until after the decommissioning of the nuclear facility. Such challenges are country specific and include, but not limited to, issues related to the legal system, labor/employment laws, regularity framework, personal performance, trustworthiness, insider threat and other issues that are different from one country to the other. The objective of this paper/presentation is to highlight such challenges to nuclear security in newcomer states and suggest ways on how to address them in nuclear security education and training programs and include case studies from other sensitive industries, within the country, that share with nuclear similar types of threats.

State

Jordan

Gender

Male

Primary author: MALKAWI, Salaheddin (Jordan University of Science and Technology)

Presenter: MALKAWI, Salaheddin (Jordan University of Science and Technology)

Track Classification: PP: Newcomers to nuclear power and research reactors: opportunities and challenges
Establishing a nuclear security inspection programme in Morocco

The Kingdom of Morocco has been using, transporting and storing, for decades, radioactive sources in a variety of socioeconomic sectors, and different practices. It also had established a legal and regulatory framework for nuclear and radiological safety since 1971. However, security aspects were not addressed at that time.

The Kingdom of Morocco has been, like many countries, facing a real and increased terrorist threat since the 2003 Casablanca terrorist event. Subsequently, it became clear that nuclear and other radioactive material could be targeted through illegal transfer, unauthorized removal, theft and/or sabotage. Therefore, and since then, different authorities and organizations started working with the objective of enhancing the security of radioactive sources within Kingdom of Morocco.

In addition, to these operational improvement, the Kingdom of Morocco has enacted, in 2014, a new law addressing nuclear and radiological safety and security, and nuclear safeguards; and the creating a unique and independent regulatory body reporting to the Prime Minister: the Moroccan Agency for Nuclear and Radiological Safety and security (AMSSNuR). Dedicated regulations on security of cat 1, 2&3 radioactive sources during use, storage and transport have been, since then, prepared and submitted to the government for approval. Other regulations on physical protection of nuclear material and facilities have been also drafted and reviewed by IAEA experts. A variety of guides dedicated to operators, to help them implementing provisions of the legal and regulatory framework, have been or are being drafted.

In order to strengthen nuclear security at the national level for authorized activities and facilities, there are two main components: the licensing process and the regulatory inspection and enforcement process.

As most countries establishing or considering the establishment of a regulatory inspection programme for nuclear security for the first time, there is a need to learn from other States or International Organizations that have years of experience in the field. This could be done, inter-alia, through workshops and/or experts missions. However, to train inspectors, the best way would be their participation through internships or technical visits in field inspections in these countries as observers. For obvious reasons, in most cases it is not doable.

The paper presents and analyses the actions undertaken and the challenges faced by the regulatory body AMSSNuR in establishing a regulatory inspection programme taking into account the preparation of inspection and enforcement procedures as part of AMSSNuR’s Integrated Managements System, guidance for inspectors and checklists as well as ensuring training and qualification of future nuclear security inspectors. This programme considers, in addition, the interface with safety and safeguards.

State
Morocco

Gender
Primary authors: Dr MRABIT, KHAMMAR (MOROCCAN AGENCY FOR NUCLEAR AND RADIOLOGICAL SAFETY AND SECURITY); BOUSTANI, bouchra (Moroccan Agency for Nuclear and Radiological Safety and Security)

Presenter: BOUSTANI, bouchra (Moroccan Agency for Nuclear and Radiological Safety and Security)

Track Classification: CC: National nuclear security inspections: training of inspectors, development of procedures and managing findings
Vitalant’s Irradiator Project Plan to Transition from Gamma to X-ray

Content:
Abstract title: Vitalant’s Irradiator Project Plan to Transition from Gamma to X-ray

Vitalant is a non–profit blood provider, which consists of 7 divisions with 127 donation centers and 18 manufacturing sites, and distributes blood and blood products to over 1,000 hospitals and health care partners across the United States. The Vitalant enterprise utilizes 24 Gamma irradiators to reduce or inactivate white blood cells, which are associated with the transmission of Transfusion-Associated Graft-Versus-Host-Disease, TA-GVHD. As a large number of the Vitalant’s Gamma irradiators were posed for resourcing and there is a potential threat of malicious use of Gamma radioactive sources, a cross-functional Irradiator Work Group was established to develop a recommendation in regards to the replacement of Gamma irradiators with x-ray irradiators. X-ray blood irradiators are considered a practical alternative to Gamma irradiators in providing an equivalent reduction/inactivation of white blood cells in blood and blood products. X-ray blood irradiators are approved by the Food and Drug Administration (FDA) and have been available for many years with numerous countries across the globe already completing this transition. The Irradiator Work Group was responsible for identifying any upcoming changes in the Federal Regulations as they applied to Gamma source blood irradiators, completion of a cost-benefit analysis of Gamma vs. x-ray, equipment selection, installation requirements, and an equipment replacement plan in which the current equipment was ranked based upon six critical factors. Per the group’s recommendation, Vitalant Executive Leadership approved the transition from Gamma blood irradiator to x-ray blood irradiators.

A contract between Vitalant and the Department of Energy/National Nuclear Security Administration’s Office of Radiological Security (ORS) was established for the removal of the Gamma irradiators and to cover the expenses incurred as a result of the source removal. ORS also provided an incentive which covers a portion of the costs of the new x-ray blood irradiators. The support from ORS was critical in ensuring that Vitalant as a non-profit blood provider would be able to decrease potential security threats while continuing to provide cost-effective blood and blood products to our patients.

The Vitalant Irradiator Work Group’s project development process, the enterprise’s progress to date on this three- year plan, and the lessons learned will be shared in this poster.

State
United States

Gender
Female

Primary author: Mrs MORRIS, Connie (Vitalant)
Presenter: Mrs MORRIS, Connie (Vitalant)
Track Classification:  CC: Innovative technologies to reduce nuclear security risks and improve cost effectiveness, where feasible
Safety and Security for small modular nuclear reactors (SMRs)

In the past decade, there have been significant developments in Small Modular Reactor (SMR) technology. SMRs range from approximately one-third the size of current nuclear power plants or about 300 MWe, to as low as 5 MWe. SMRs are promoted as economically competitive alternatives to large Nuclear Power Plants for electrical power production and other applications. The advantages of SMRs arise from being simpler and modular, carrying smaller financial risk, more adaptable for load following demands, factory production, and applicability for off-grid applications. SMRs feature simplified, compact designs, which typically include built-in passive safety systems, limited on-site refueling, and provisions for remotely monitored operation and reduced on-site staffing. A number of SMRs concepts have been proposed by various international companies for pre-licensing design review and eventually construction in Canada.

Traditional nuclear safety and security analyses and design are impacted by the proposed advanced fuel types (liquid metal, gas-cooled and molten salt), and understanding their proliferation, control, and monitoring aspects. Other challenges for SMR safety and security include: geographic isolation and distribution, lack of strong thermal or radiation signatures, lack of access to core for monitoring, aqueous fuel forms, harsh environmental conditions, tools for comprehensively assessing proliferation resistance (e.g., proliferation resistant fuels), and cyber security considerations for remote monitoring/control (e.g., anomaly detection, secure data transmission...). This paper discusses these considerations and describes possible strategies for these novel facets of SMR concepts.

State
Canada

Gender

Primary author: Dr BENTOUMI, Ghaouti (Canadian Nuclear Laboratories)
Co-authors: Dr CHAUDHURI, Ankur (Canadian Nuclear Laboratories); Dr VAN DER ENDE, Bryan (Canadian Nuclear Laboratories); Dr BHASKAR, Sur (Canadian Nuclear Laboratories)
Presenter: Dr BENTOUMI, Ghaouti (Canadian Nuclear Laboratories)

Track Classification: PP: Nuclear security of new nuclear technologies (e.g., small modular reactors)
THRUSTWORTHINESS PERSPECTIVE IN THE INTEGRATION OF NUCLEAR COMPUTER SECURITY INTO STATE’S CYBERSECURITY REGULATION IN INDONESIA

Nowadays, Indonesia has three research reactors managed by National Nuclear Energy Agency of Indonesia (BATAN) which located in Yogyakarta, Bandung and Serpong. The reactors were not constructed based-on digital technology, therefore we are not worrying about cyber attacks. However, in the near future Indonesia plans to build a prototype of advanced small nuclear power plant. The latest technology employed in an advanced nuclear power plant usually based-on digital technology. Therefore, the problem of nuclear computer security should be considered as well. From nuclear computer security point of view, Indonesia do not have a specific regulation on nuclear computer security. Indonesia currently has BAPETEN Chairman Regulation (BCR) no 3/2011 on the Nuclear Reactor Safety Design and BCR no 5/2011 on the Maintenance of Non Power Reactor. These BCRs has no specific item describing about nuclear computer security. Even though IAEA document NST 045 on Computer Security on Nuclear Security described that the state should develop and maintain a national computer security strategy as part of its nuclear security regime, and the state should designate a competent authority to lead responsibility in the development of the strategy.

Ministry of Communication and Information - Republic of Indonesia, as leading sector in the field of Telecommunications and Information and national information security managers and policy has the role as reference for the formulation of a national strategy road map on cyber defense. They have five cyber security policy agendas in establishing a Secure Cyber Environment, through implementation of strategy models “Ends-Ways-Means” which focus on measurable goals, priorities and actions. Based-on the strategy cyber defense must be systematically coordinated and integrated. It cannot be treated as sporadic and casuistry. Therefore, the acquisition and utilization of technology, including information technology especially in the nuclear area, should have to be able to speed up, simplify and ensure the completion of the strategic problems of the nation and the State. Up to now, cyber defense application in Indonesia still has not become a national initiative coordinated. Implementation steps remains sectoral and based on the interests and abilities of each. Capability and deterrence and prevention, and recovery were still weak, so it is still very vulnerable to attack that is massive. Several initiatives have been undertaken by agencies and corporate institutions in order to implement cyber defense that has been done such as (a) Ministry of Communication and Information established the Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTI) in 2007, (b) National Code and Cyber Agency has a unit that specializes in securing ICT resources, especially with regard to Signal Intelligence.

Indonesia as a multi culture nation has hundreds of subculture which provides great effects to the nuclear security and also nuclear computer security. Culture differences and characters do not want to understand differences will be a source of suspicion and distrust between personnel in an organization. Conflict between communities with differences in for example political group will lead to destruction and riot. The destruction can occur everywhere including in nuclear computer security environment.

IAEA document NSS-13 describes that the State laws, regulations, or policies regarding personal privacy and job requirements should determine the trustworthiness policy intended to identify the circumstances in which a trustworthiness determination is required and how it is made, using a graded approach. The trustworthiness is implemented to persons with authorized access to sensi-
This paper describes design of nuclear computer security regulation which will be integrated to the state's cyber security regulation. The new regulation will emphasize on how to anticipate the weaknesses of trustworthiness due to the existence of multi culture in Indonesia. Base of the regulation is the Act No.11/2008 on Information and Electronic Transactions (ITE Law) and Government Regulation No. 82/2012 on the Implementation of Electronic Transactions and Systems as foundation to build national Cyber Security and Cyber Defense Security. The regulation will be constructed sequentially in 2 steps, conceptual step and drafting step. This paper explains the regulation in the state of conceptual step. Framework of Government Regulation in Indonesia includes (a) title, (b) introduction, (c) core, (d) closing. The title is about Government Regulation on “Nuclear Computer Security to Strengthen the National Cyber Security”. Introduction will discuss on background, scope, objective, benefit, structure, definition. The core includes chapters on (a) Concept and Context, (b) Roles and Responsibility of State, (c) Roles and Responsibility of Stakeholders, (d) Establishing the State on Cyber Security, (e) Establishing the Nuclear Computer Security Strategy, (f) Establishing the Nuclear Computer Security Culture, (g) Implementation of Nuclear Computer Security, (h) Improvement of Nuclear Computer Security Plan, (i) Sustaining of Nuclear Computer Security. The closing will discuss on sanction. We hope that the Government Regulation will strengthen the nuclear computer security to protect the public and environment from the utilization of nuclear energy in Indonesia.

Keywords: trustworthiness, nuclear computer security, cyber security, regulation, Indonesia

**State**

Indonesia

**Gender**

Male

**Primary author:** NUGROHO, Djoko Hari (BAPETEN)

**Presenter:** NUGROHO, Djoko Hari (BAPETEN)

**Track Classification:** PP: Insider threats
Evaluation of the interface between safety, security and safeguards in the legislative and regulatory framework: A national approach

Synopses:
Establishing and sustaining an effective and credible regulatory body is ensured through, inter alia, continuous improvement. In this sense, AMSSNuR has established an internal scientific committee whose mission is among others to assess and make proposals to AMSSNuR for improving its activities the national, regional and international levels. In this respect, AMSSNuR has conducted a self-assessment in order to assess its performance, against established international standards and guidance, and to identify areas for improvements.

The self-assessment process is as follow:
- Preparation of the questionnaires:
  The internal assessment is performed accordingly to the IAEA Self-Assessment of the Regulatory Infrastructure for Safety (SARIS) as required by the scientific committee. It has the aim to assess the safety legislative and regulatory framework based on the requirements of GSR part1 (Rev.1): Governmental, Legal and Regulatory Framework for Safety, section 2: Responsibilities and functions of the Government. The Department of Nuclear Security and Safeguards of AMSSNuR has the duty to assess the Requirement 12: Interfaces of Safety with Nuclear Security and with the State System of Accounting for, and Control of Nuclear Material.
- Answering the questionnaires:
  In the form of a check list, the self-assessment contains 7 questions on the interface of safety with nuclear security and safeguards on different areas as follow: the institutional infrastructure; roles and responsibilities in the legal and regulatory framework for the assessment of safety and security; responsibilities for oversight and enforcement; liaison with law enforcement agencies; integration of emergency response arrangements for both safety related and nuclear security related incidents; implementation and integration by design of security and safety measures; and planned measures to ensure adequate infrastructural arrangements for the interface between safety and security.
  The IAEA has defined specific requirements to assess those areas so that the law no.142-12, the draft decree on security of radioactive sources, the draft decree on safeguards implementation, the draft decree on physical protection of nuclear materials and facilities, the draft decree on emergency preparedness and response, and the draft decree on nuclear safety were assessed to see if the legislative and regulatory provisions takes into consideration the interface between safety, security and safeguards.
- Analyzing the questionnaires:
  Once all questions were answered, the questionnaire was sent to the scientific committee for analyzing, making conclusions on the findings and defining areas needing improvement.
- Developing an improvement action plan:
  The next step is to develop an action plan with the aim to seek improvement of the identified gaps and weaknesses within the regulatory framework.
- Making follow up:
  after the implementation of the action plan, follow up activities will be performed including indicators on how the implementation of the plan is going to affect the regulatory performance of AMSSNuR.

It is worth mentioning, the Moroccan legislative and regulatory framework generally addresses the interface between safety, security and safeguards. The internal self-assessment described above
is an important tool that allows AMSSNuR to assess its regulatory capabilities and to ensure the development and the sustainability of safety, security and safeguards.

State

Morocco

Gender

Primary authors: Ms LASFAR, ASSIA (Moroccan Agency for Nuclear and Radiological Safety and Security); Ms MOUSSAID, KHADIJA (Moroccan Agency for Nuclear and Radiological Safety and Security)

Presenter: Ms LASFAR, ASSIA (Moroccan Agency for Nuclear and Radiological Safety and Security)

Track Classification: CC: Nuclear safety and security interfaces
Sensitive detection of special nuclear materials based on gamma-fast neutron coincidence counting for RPM application

The detection of special nuclear materials (SNM) is one of the main goals of the nuclear security chain, and Radiation Portal Monitors (RPMs) are extensively used to achieve this goal. These systems are designed to compare the measured neutron and gamma-ray counting rates with a predefined counting level when objects and/or persons passing through them, and set an alarm if the radiation rates are above a predefined level. The alarm level needs to be related to the normal background radiation and how background events may trigger false alarms due to statistical fluctuations is a critical point for the design of RPM systems. The higher the specificity of the sensor signals used for determining the alarm criteria the higher will be the “signal-to-background” ratio and consequently the lower will be the resulting false positive rate. At the same time the sensor efficiency must be high enough for optimum sensitivity.

The majority of RPMs designed to detect neutrons makes use of He-3 proportional counters or, to a lesser extent, organic scintillator detectors. Due to the global shortage of He-3 there is an increasing focus on He-3 free systems. Although both detector categories have proven to be efficient in detecting nuclear and radioactive materials, there are important issues related to “nuisance” alarms and difficulties in detecting small quantities of SNM, in particular in shielded environments, reported in the literature. A novel approach that addresses these issues utilizes the high multiplicity and short time-of-flight of gamma rays and their short time correlations with fast neutrons as a unique signature of materials that undergo spontaneous or induced fission, such as SNM. Making use of gamma-fast neutron coincidence counting as an additional detection modality in parallel with standard singles gamma and neutron counting the system sensitivity can be increased significantly, while neutron-neutron coincidence counting often is prohibitively inefficient. Efficient imaging of SNM materials within the field of view is also made possible using the gamma-fast neutron detection mode. Moreover, the use of coincidences adds to the system the capability of quantifying the material in question, expanding the applications from prevention of nuclear material trafficking to accountability and control.

Computational simulations are very useful and well accepted in the scientific community in order to investigate development setups and improve detection systems setups before mountain them. The theoretical accuracy in simulate nuclear fission, decay and radiation interaction with matter make Monte Carlo simulations codes a powerful tool in the area of nuclear security. This paper performed computational simulations to investigate the use of fast neutron and prompt gamma-ray coincidences detection in scintillators and the code MCNP (Monte Carlo N-Particle), version 6.2. was used. Spontaneous and induced fission including neutron, gamma-ray multiplicity and correlations were taken into account. Pulse Shape Discrimination (PSD) is the method applied to distinguish between neutron and photon pulses in the scintillator detector signal. In the computational environment the scattering of photons and neutron coming from the same fission event were counted as coincidences, when found inside different detectors in a pre-defined time window were counted as coincidences. The RPM prototype was modelled as double sided with two detectors assemblies containing four scintillator detectors each. The standard ANSI N42.35-2016 was used to define the RPM design and the source positions to perform the simulation. Count rates for single gammas, single neutrons, neutron-neutron and gamma-neutron coincidences were calculated and compared for the standard Cf-252 source and PuO2 samples in bare and shielded conditions. The detection zone was determined and a 3D map of counting rates percentage constructed. A discussion addressing the positive alarm threshold definition - as function of sigma and its multiplier factor - including particle miss-classification related to PSD in scintillators detectors is also presented.
The results showed high single-neutron and gamma-fast neutron coincidence rates. The latter was calculated being at least 10 times higher than the neutron-neutron coincidence rate in the bare source condition. The sigma multiplier factor for gamma-neutron coincidences was found to be significantly higher than the one calculated for single-neutron detection and the difference in performance was further increased in the presence of high-density polyethylene (HDPE) shielding. The novel method of gamma-neutron coincidence detection provided reasonable detection rates in the investigated setup even for small samples of SNM of the order of a gram and short inspection times of a few seconds. It provides a clean signature for SNM, promising to enhance the performance of future RPM systems significantly above the current state-of-the-art. Experimental studies of the prototype system will also be reported.

**State**

Sweden

**Gender**

Female

**Primary authors:** TROMBETTA, Débora (KTH); Prof. CEDERWALL, Bo (Royal Institute of Technology (KTH))

**Presenters:** TROMBETTA, Débora (KTH); Prof. CEDERWALL, Bo (Royal Institute of Technology (KTH))

**Track Classification:** MORC: Preventing illicit trafficking of nuclear and radioactive material
Examining Cyber Security Vulnerabilities and Counter-Measures to Combat the Insider Threat in Radiological Security

The U.S. Department of Energy/National Nuclear Security Administration’s Office of Radiological Security (ORS) collaborates with partner countries throughout the world to enhance the security of radioactive sources used for legitimate purposes. The partner stakeholders’ environments consist of operators utilizing ionizing radiation for medical, industrial, and research applications. In each of those domains, the risk of an insider is ever-present within the spectrum of threats and threat agents. With the continued advancement of security technology and the proliferation in the use of networked security components in recent years, previously unforeseen capabilities are being leveraged by security practitioners to greatly enhance detection, assessment, and response security functions. However, as systems increase in the level of integration and complexity, such as those either connected to or riding directly on a site’s Information Technology (IT) network, those same security practitioners must also remain vigilant of the associated risks.

IAEA Nuclear Security Series No. 11, Security of Radioactive Sources, outlines security objectives for the various security functions of detection, delay, and response. NSS-11 also emphasizes the importance of understanding the threat environment, including the threat posed by the insider, by conducting a vulnerability assessment at a site. Due to the purposes for which radioactive materials are used in several common application spaces, such as medical treatment, academic research, and industrial applications that emphasize process throughput, the quantity of people who have access to the source (whether escorted or unescorted) presents a security management challenge.

As the security components become further networked and interrelated, satisfying the recommendations of NSS-11 necessitates a greater emphasis be placed on insider mitigation through the strategic identification, selection, and implementation of administrative, technical, and physical controls to address the cyber vulnerabilities.

To ensure detection of unauthorized attempts to access the radiological source and to counter the insider threat in an environment where it is challenging to limit access to the source, it is necessary to seek new counter-measures. Technological solutions continue to become increasingly affordable, leading to new options for augmenting source security and improving sites’ ability to address IAEA recommendations regarding security management and access control, as well as the security fundamental of adversary detection. Unfortunately, as security measures evolve, so does an adversary’s capability to defeat those measures. Off-site monitoring of security alarms provides some assurance that an insider’s attempts to gain unauthorized access to the source will be detected and a response initiated. Off-site monitoring is, in its turn, dependent upon reliable communications via a variety of channels that may include telephonic, internet, and cloud-based options.

Because of the networked nature of security system hardware and the need for reliable communication to be effective, security system design and deployment must consider physical security from a cyber-security perspective. Key first steps include a range of procedural and practical measures to close fundamental gaps in cyber security and enable the successful employment of networked security systems to prevent malicious acts. Establishing multiple channels of communication, as well as the standard defense-in-depth approach to security system design combine to mitigate the threat posed by a cyber-based attempt to thwart the security system, as well.

NSS-11 identifies the security functions of detection, delay, and response to be addressed by an effective security systems to address the threats to radioactive sources. The recommended response objectives captured in Table 2 of the document hinge on provision of immediate response to an alarm in order to satisfy the recommended requirements. In its interaction with responders to improve response capabilities, expediting data flow to the responders themselves is frequently identi-
fied as a mechanism to satisfy those requirements. In the course of collaboration, ORS has striven to identify a mechanism to further fortify the mechanisms for ensuring data flows expeditiously to necessary response personnel. One solution being explored is the development of a cloud-based architecture to streamline communications, ensure delivery of alarm notifications and key data, and ultimately optimize the response timeline and maximize the possibility of interrupting the adversary. This paper will specifically survey the challenges posed by the cyber vulnerabilities at the facilities using radiological sources, the measures identified to mitigate those challenges, and the persistent problem areas that still demand solutions. Additionally, the paper will specifically survey the cyber-security challenges posed by the use of the cloud-based solutions being explored to optimize the ability of sites and responders to achieve the security objectives defined in NSS-11 regarding detection, delay, and response to malicious attempts to access a radioactive source.

State
United States

Gender
Female

Primary author:  Ms WISE, Jaime (Pacific Northwest National Laboratory)

Co-authors:  HAZEL, Michael (Pacific Northwest National Laboratory (US Department of Energy)); Mr GORTON, Brandon (Pacific Northwest National Laboratory); Mr HIGGINS, Brian (Pacific Northwest National Laboratory)

Presenter:  HAZEL, Michael (Pacific Northwest National Laboratory (US Department of Energy))

Track Classification:  PP: Insider threats
Implementing Sustainability Programme: Lessons Learnt from the U.S.-Russian Nuclear Security Cooperation

INFCIRC/225 “The Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities” is key IAEA document defining objectives and elements of a State’s physical protection regime. Its latest revision, INFCIRC/225/Revision 5 issued in 2011, first introduces concept of sustainability into physical protection activity. In particular, it recommends that “The State should establish sustainability programme to ensure that its physical protection regime is sustained and effective in the long term by committing the necessary resources”. It further recommends that “Operators, shippers and carriers should establish sustainability programmes for their physical protection system” and lists elements of sustainability programme. The issue of sustainability first became part of nuclear security agenda within the framework of nuclear security cooperation between the United States and Russia. This cooperation started shortly after the collapse of the Soviet Union and was aimed at improving nuclear security at Russian nuclear facilities, as well as developing national nuclear security infrastructure. Major source of funding was the United States federal budget, as economic conditions in Russia did not allow financial support for nuclear security adequate to the challenge. This led to the situation, when maintenance and upgrade of nuclear security in Russia became highly dependent on the U.S. funding support and concern arose re Russia’s own capability to upgrade and maintain proper level of nuclear security after withdrawal of the U.S. funding support. To address this challenge a concept of sustainability was introduced and a range of projects was initiated aimed at ensuring that nuclear security in Russia is sustainable and Russia has all the necessary capabilities to independently maintain and improve nuclear security over indefinite period of time. Similar efforts were implemented within the framework of other technical assistance programs implemented by the U.S. in other countries. While development of physical protection systems in countries that were not part of the nuclear security cooperation with the U.S. might follow different path and face different issues, effort to develop sustainable nuclear security in Russia can provide multiple lessons that can be used in implementing sustainability recommendations of INFCIRC/225/Revision 5. This paper will review experience of developing sustainable nuclear security in Russia and identify lessons that can be used in implementing sustainability programmes in other countries following IAEA recommendations.

State

Russian Federation

Gender

Primary author: KOVCHEGIN, Dmitry (Independent Consultant)

Presenter: KOVCHEGIN, Dmitry (Independent Consultant)
Track Classification: CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
Nuclear Security in Slovak Republic

Regulatory oversight for nuclear security: practices and challenges

The Nuclear Regulatory Authority of the Slovak Republic (UJD) is responsible, inter alia, for state supervision upon nuclear safety and physical protection. In recent years we have been facing new challenges and practices, changes in threat environment and new threats have to be taken into consideration, when carrying out our obligations / duties. This article describes the most recent changes.

The nuclear security legislation lags behind the requirements on nuclear security in two to three years. The main reason for this lag lies on one hand in a long and complicated legislative process, on the other hand in rapid changes in requirements for nuclear security. The UJD is at present drafting new legislation which reflects the requirements from the Amendment to CPPNM and also in some new areas.

Based on the fundamental principle G the UJD prepares annually state’s Threat Assessment and Design Basis Threat. These document reflect besides “classic” threats also newly arisen threats. The UJD also deals with new views on nuclear security and its interactions mainly with nuclear safety and emergency response and preparedness.

One of the most rapidly growing threats is misuse of unmanned aerial vehicles (drones). Drone may be used for several types of malicious acts, for theft, sabotage and also for monitoring of physical protection system and helping the adversaries when performing their tasks. Slovak government established and founded a working group which is responsible for the preparation of countermeasures against the use of drones in critical infrastructure objects and nuclear installations. At present the process of the selection of effective anti-drone systems is underway.

Cyber threat represents for nuclear/cyber security one of the most difficult challenges and a dangerous topic. Classic cyber security (administrative systems cyber security, internet security, ...) is not sufficient enough to eliminate all the threats faced by nuclear installations today. When planning the cyber threat countermeasures, the operators of nuclear installation in Slovakia focus on three main tasks. The first task is cyber security of physical protection systems itself, the second task is protection of operational and emergency control systems and protection of sensitive information.

Protection against plane crash became relevant some years ago. It represents a difficult task for the physical protection system and could be defined as a threat beyond the design basis threat. Two units of the nuclear power plant under construction in Mochovce are equipped with protection of some important systems against intentional attack by small aircraft. The UJD also requires that the planning and design of the project of interim spent fuel storage facility capacity extension is designed against an accidental crash of an airliner, or deliberate attack with an airliner.

New threats in nuclear security area have highlighted the issue of the effectiveness of physical protection systems. For the evaluation of physical protection systems, we use SAVI and EASI software. However, this software does not calculate the probability of neutralization of attackers. The UJD has developed a new calculation tool which can perform a calculation of probability of detection as well as probability of neutralization.

Physical protection system effectiveness represents technical part of an effective physical protection system. Equally important for the effectiveness of physical protection system is nuclear security culture as a part of organizational culture. The UJD in co-operation with the operators evaluate the level of nuclear security using self-assessment described in IAEA’s document NSS No. 28 – T, Self-assessment of Nuclear Security Culture in Facilities and Activities.
Common aim of nuclear safety and nuclear security is protection of persons, assets, society and the environment from the harmful effects of ionizing radiation. However, the ways how they achieve its goal are different. The UJD actively participates in international meetings dealing with nuclear safety – nuclear security interface. The UJD sees possible benefits and synergies in this area, though it is important to see the equal importance of nuclear safety and nuclear security. New threats and new challenges in nuclear security area request also new approaches from regulatory organs. It is imperative that the regulator responds in a timely manner to the new realities, and it is also necessary to modify the legislation accordingly.

State
Slovakia

Gender

**Primary author:** Dr VACLAV, Juraj (Nuclear Regulatory Authority of the Slovak Republic)

**Presenter:** Dr VACLAV, Juraj (Nuclear Regulatory Authority of the Slovak Republic)

**Track Classification:** PP: Nuclear security of nuclear fuel cycle facilities: emerging technologies and associated challenges and complex threats
STRENGTHNING THE GLOBAL SECURITY: THE ROLE OF NATIONAL, REGIONAL AND INTERNATIONAL COOPERATION

Nuclear and radiological techniques and applications are used in our daily life, including medicine, industry, agriculture, energy, research and others. However, they cannot be sustained if not safe and secure. It is widely recognized, that nuclear and radiological threat is real, global and is increasing.

The IAEA and other regional and international partners have been, for many years, promoting, at the request of Member States, nuclear security nationally, regionally and globally. To strengthen these efforts, the U.S. President Obama, during his speech in Prague, 2009, described nuclear terrorism as “the most immediate and extreme threat to global security” that should be prevented. In this respect, he invited the international community to secure vulnerable nuclear and other radioactive material against the evolving threat towards them and announced the launching of the nuclear security summit with three main goals: reducing the amount of dangerous nuclear material in the world; improving the security of all nuclear material and other radioactive sources; and improving international cooperation. To sustain and continuously improve nuclear security, the IAEA organized for the first time an International Conference on Nuclear Security with a ministerial segment and a technical programme that has been repeated in 2016 and will be held for the third time in 2020, making the IAEA playing the central and essential role in coordinating global efforts in nuclear security globally.

The Kingdom of Morocco, enacted in 2014 the law no. 142-12 that covers Safety, Security and Safeguards, and created an independent Regulatory Authority named the Moroccan Agency for Nuclear and Radiological Safety and Security (AMSSNuR) which became operational in October 2016.

Since its creation, AMSSNuR has been very active in developing mechanisms of cooperation at different level, through the establishment of many Memorandums of Understanding (MoU) with international and regional players and with sister regulatory authorities and different organizations working in the same field. These MoUs aim at strengthening the cooperation between the Kingdom of Morocco and other countries and Organizations in terms of exchanging information, experiences and lessons learned in the fields of nuclear and radiological security.

AMSSNuR, assigns high priority to cooperation at regional and international levels. In this paper we will share the approach adopted by AMSSNuR in the development and implementation of mechanisms of cooperation at regional and international levels.

State
Morocco

Gender

Primary authors: Dr MRABIT, KHAMMAR (MOROCCAN AGENCY FOR NUCLEAR AND RADIOPHYSICAL SAFETY AND SECURITY); Mr LAGHOUAZI, TAHA (MOROCCAN AGENCY FOR NU-
CLEAR AND RADIOLOGICAL SAFETY AND SECURITY): Ms ASSEM, CAMELIA (MOROCCAN AGENCY FOR NUCLEAR AND RADIOLOGICAL SAFETY AND SECURITY)

**Presenter:** Dr MRABIT, KHAMMAR (MOROCCAN AGENCY FOR NUCLEAR AND RADIOLOGICAL SAFETY AND SECURITY)

**Track Classification:** CC: Information and computer security considerations for nuclear security
STUDY ON THE IMPLEMENTATION OF NUCLEAR FORENSICS IN VARIOUS LEGAL SYSTEMS

All illicit activities concerning nuclear or other radioactive materials found outside of regulatory control (MORC) insofar as they are sanctionable by the criminal law, should be followed by a criminal investigation and possibly prosecution, depending on the legal requirements applicable in that specific jurisdiction. Given the seriousness of the offences regarding MORC and the potential dangers posed by such materials, as recognized and required by various international legal instruments such as CPPNM and ICSANT, specific deeds involving nuclear or other radioactive materials should make object of criminal proceedings, which can also provide the basis for exchange of information and international cooperation.

Nuclear Forensics provides the essential tools for unfolding the criminal investigations and prosecutions where nuclear or other radioactive materials are concerned. IAEA recommends that member states develop nuclear forensics capabilities according to their nuclear security related needs NSS15. However, after such needs are identified and technical capabilities are established, it can prove challenging to actually implement Nuclear Forensics as a functional tool to prevent and respond to Nuclear Security Events on a national level. The reason for this is the specificity of legal provisions in national law systems.

This paper presents the legal requirements that have to be taken into consideration during the implementation of Nuclear Forensics within the national legal framework of a state, with the purpose to collect, analyse and interpret evidence of illicit activities involving nuclear or other radioactive materials found out of regulatory control. It provides an overview of the main role of Nuclear Forensics within the criminal investigation while focusing on the specificity of the Civil vs Common law systems. We also look into the roles and responsibilities of the main stakeholders in criminal investigations in the different legal systems and how that might influence the nuclear forensics’ integration and valorisation in the overall national security system. The study of the successful implementation of nuclear forensics in Romania will offer a good example of the development of such capabilities and how to bring them into effective action in accordance with the national framework.

By way of reviewing the literature and comparing various legal frameworks that apply to different legal systems worldwide, we endeavour to demonstrate that, when implementing new scientific tools like those offered by Nuclear Forensics within the scope of the criminal investigation, the peculiarities of various legal systems have to be taken into consideration. While some of the same fundamental principles are at the basis of both Civil and Common Law, they evolved separately and have their own legal structures and rules of procedure, even though throughout history the two systems obviously influenced one another. Nuclear forensics plays an essential role in the efforts which states undertake during the response and prevention of nuclear security events. In order to be effectively used for the purpose of criminal proceedings, it has to be implemented in an effective legal way, in accordance with national legal requirements, following the same legal principles and procedures as those applying to traditional forensics.

1 NSS15, IAEA, Vienna (2011)
2 The common law and civil law traditions, 2010 Berkeley University, The Robbins Collection, retrieved online on 20.11.2018

State

Romania

Gender
Male

**Primary authors:** Dr APOSTOL, Andrei I. (Horia Hulubei National Institute for Physics and Nuclear Engineering (IFIN-HH), Bucharest-Magurele, Romania); Mrs DINU, Elena (Directorate for Investigating Organized Crime and Terrorism (DIICOT), Bucharest, Romania)

**Presenter:** Dr APOSTOL, Andrei I. (Horia Hulubei National Institute for Physics and Nuclear Engineering (IFIN-HH), Bucharest-Magurele, Romania)

**Track Classification:** MORC: Nuclear forensics
Building Capacity in Training Capabilities Nuclear Security Support Center Network Working Group C

The world moves at a very fast pace nowadays, and with it, new threats start to emerge and some of them come from the most unlikely sources. The whole world currently faces a common enemy, one that knows no boundaries, has no limits, has no fear. And this is the most dangerous enemy there is: the one which fears no death and whose only goal is to destroy, to inflict terror and make everyone feel helpless. This enemy is everywhere, and will take any resource necessary to fulfill its goal.

Communication and coordination among agencies, and among countries is a key element in responding to an incident. So communication protocols and channels have to work effectively, they have to be always on alert and ready to be activated, they have to have a clear understanding of which steps to take in order to manage the incident. And these mechanisms have to be developed among the involved actors, they have to be put to practice, and the best way to become proficient in responding is to train and exercise. Exercises have to be carried out on a daily basis, both tabletop exercises and field exercises are the most useful resource in order to test every protocol, and detect flaws and work in their solution.

And, since the threats are now global, recognize no borders and have no limits, they must be dealt with in that same spirit: with no boundaries, with no fear of the unknown. This is why Argentina and Hungary, like many other countries in their own national capacity, are developing its Supports Centers. These Centers are part of the International Network for Nuclear Security Training and Support Centres of the IAEA. The Network has 61 member states. The reason why it is important to be part of such a network is because it is the best way to learn from each other, to share information, to share experiences and best practices, to develop training strategies together, to learn about new ways to tackle with new threats, and to create a collaborative network that -at some point- would be able to do cross trainings between countries.

The training facility that is being currently designed is destined to work on the following areas: Basic practical radiation knowledge; Security and Safety in transport of radioactive sources and other nuclear and radioactive material; Perimeter nuclear asset custody and guard; Preparedness and safeguarding of crime scenes involving nuclear or radioactive material for forensic analysis; Cybersecurity and new threats; Human Resource Management in order to combat insider threats; Force on force adversaries combat; Tactical communications while on patrol; Fixed site security; Security drills; Intrusion detection time-lines; Set up and use of detection instruments and technology; Configuration and use of delay barriers.

Since March 2019, Argentina and Hungary chair the Working Group C of such network, which is in charge on Information Sharing, Promotion, and Outreach is to strengthen information sharing among NSSCs and help raise awareness of Network Member training courses and other activities. Maintaining and enhancing a database of all NSSC Network Members, to include search functions, key statistics, and a map of NSSCs by operational status, capabilities, and technical specialization. Facilitating the sharing, promotion, collation and dissemination of information related to nuclear security training and other activities carried out by NSSC Network Members through a NSSC Network events calendar. Monitoring use of and improvements needed for the NSSC User Group on the NUSEC Portal. Carrying out regular analysis of data contained in the NSSC Network events calendar and database and sharing a summary of this analysis at the Annual Meeting and Leadership Meeting, and coordinating development of each edition of the NSSC Network Newsletter and other outreach materials, working in close cooperation with the IAEA Secretariat. These tasks are crucial to develop proper training on nuclear security and be able to response to a possible event.
State
Argentina

Gender
Male

Primary author:  BIEDA, Tomas (Ministry of Energy and Mining)
Co-authors:  KOVACS-SZELES, Eva (Hungarian Academy of Sciences, Centre for Energy Research);  CÁCERES, L Federico (Undersecretariat of Nuclear Energy)
Presenter:  BIEDA, Tomas (Ministry of Energy and Mining)

Track Classification:  CC: Role of Nuclear Security Support Centers to support and sustain national nuclear security regimes
Strong nuclear security framework as an essential element of nuclear new-build programme

Establishment of the robust legislative and institutional framework for nuclear power sector, adequately addressing nuclear security, remains one of the main challenges faced by countries embarking on nuclear power. From this point of view, the aim of the paper is to present good practices and lessons-learned by Poland in that field during implementation of its nuclear power programme. In January 2014 Polish Government adopted Nuclear Power Programme (“PNPP”) which sees 2 nuclear power plants to be constructed in Poland by 2035 with a total capacity of 6000 MWe. The Programme is a strategic, comprehensive document that sets out the scope of measures to be taken to implement nuclear power in Poland. At the very early stage of the nuclear power programme the Government expressed its strong commitment to nuclear security. One of the Programme priorities is “to ensure the highest achievable safety/security for NPPs”. As a result Poland has been undertaking many actions to enhance its nuclear security framework, e.g. it developed its nuclear laws and hosted several missions of International Atomic Energy Agency to ensure that Polish nuclear infrastructure meets all international standards and best practices in that field. Based on Polish experiences in that field, the proposed paper will discuss various ways of how nuclear new-build countries may enhance its nuclear security framework.

The first part of the paper will present how nuclear security has been addressed in Polish Nuclear Power Programme. Chapter 6. of PNPP will be discussed in detail, in which importance is given to physical protection of nuclear facilities is highlighted: “the top priority of PNPP is to ensure nuclear safety radiological protection with respect to the public and the nuclear power facility personnel, including physical protection of any nuclear facilities”.

The second part will present the most important legal and institutional arrangements for nuclear security as prescribed in Atomic law act and secondary legislation.

The third part will outline various types of IAEA review missions, in particular International Physical Protection Advisory service (IPPAS mission), as powerful tools to enhance nuclear security framework in nuclear-new build countries. With this regards it must be noted that, within the last few years Poland hosted various IAEA missions which resulted in series of suggestions, recommendations and good practices identified in various areas of national nuclear policy and law. The most significant and interesting lessons-learned from those missions that might be applicable also in other nuclear new build countries will be presented in the paper.

In the fourth part of the paper the conclusions will be drawn up on how clear and strong commitment to nuclear security at the very early stage of implementation of nuclear power programme contributed to enhancement of nuclear security framework in Poland as a nuclear new-build country.
Primary author:  Mr ADAMCZYK, Kamil (Ministry of Energy)
Presenter:  Mr ADAMCZYK, Kamil (Ministry of Energy)

Track Classification:  CC: Implementation of national legislative and regulatory frameworks, and international instruments
Challenges in implementing and sustaining the information security policy for OAP

Office of Atoms for Peace (OAP), the nuclear regulatory body in Thailand has gone through the steps and guideline provided by IAEA of conducting an effective information security policy which shall include (i) Analysis of organizational information especially sensitive information, (ii) Information classification, (iii) Information security policy framework design and implementation, and (iv) Sustainability of information security policy. Therefore, the OAP’s information security policy and plan has then been reviewed and updated in accordance with the Nuclear Energy for Peace Act (2017) and IAEA guideline. However, the reality shows that this information security policy (ISP) has not been used effectively throughout the organization. There exists some hindrances experienced by OAP staffs in implementing and sustaining the ISP. One of them is the incoming of new evolving threats and rapid advancement of technology caused the ISP to be revised and updated more frequently to take account of such threats. Moreover, poor communication between top management and employees regarding security policy and security culture is also an obstacle resulted in the ineffective policy. In addition, an effective integrated management system which help to ensure the confidentiality, integrity, and availability (CIA) of sensitive information, as well as a robust security culture and strong security awareness program such as security training, qualification program, etc. are key factors for better sustaining the policy.

State
Thailand

Gender
Male

Primary author: MANEECHAYANGKOON, Raffin (Office Atoms for Peace)
Presenter: MANEECHAYANGKOON, Raffin (Office Atoms for Peace)

Track Classification: CC: Information and computer security considerations for nuclear security
Roles and Responsibilities of Stakeholders during a Radiological Incident: A Theoretical Case Study of Bangladesh

Ensuring security of radioactive materials used in different medical and industrial facilities is more critical than doing the same in nuclear power plants. Possessing radioactive materials in medical and industrial facilities does not house strong physical protection and response systems. Operators don’t have any official communication protocol systems to who they should contact during any radiological incident if it occurs. International terrorist organizations are well aware of the situation and may use this to their advantage. Under this inadvertent situation, the adversaries might possess radioactive elements that may be used for making dirty bombs. These bombs may be used for weapons of mass disruption which may bring about potential health and economical consequences. Bangladesh is underway to construct its first the nuclear power plant at Rooppur site. However, nuclear and radiological emergency response plan is yet to establish and newly established regulatory body is over pressure in managing the under-construction nuclear power plant. There is no legal communication protocol among stakeholders such as police, border guards, coast guards, and customs. If any radiological incident would occur in any hospitals or industries across the country, how crime scene management would be tackled out. In this work, a theoretical case study has been conducted to identify the roles and responsibilities of the stakeholders during a radiological incident. The work has tried to suggesting a communication protocol suitable for Bangladesh, i.e. whom the stakeholders should contact if an incident occurs. The work has also suggested on how the law enforcing forces should prepare them in order to face such adversities and urges to establish a special squad dedicated for these specific incidents. The way the crime scene should be managed has also been focused on. The roles and responsibilities of the State, have been identified to prevent large scale dispersion of radioactive elements within common people. The roles and responsibilities of the regulatory authorities have also been identified in order to prevent uncontrolled and unregulated use of radioisotopes. Finally, the work has suggested the duties of the operators, who are the end users of radioactive isotopes, in the face of an adverse situation like terrorist attack.

State
Bangladesh

Gender
Male

Primary author: Dr ISLAM, Md Shafiqul (Department of Nuclear Engineering, University of Dhaka, Dhaka-1000, Bangladesh)

Co-author: Mr KHAN, Abid Hossain (Department of Industrial and Production Engineering, Jashore University of Science and Technology, Jashore-7408, Bangladesh)
**Presenter:** Dr ISLAM, Md Shafiqul (Department of Nuclear Engineering, University of Dhaka, Dhaka-1000, Bangladesh)

**Track Classification:** MORC: Coordinated response to nuclear security events
DEVELOPMENT OF NUCLEAR SECURITY REGULATIONS IN GHANA

The Nuclear Regulatory Authority Act, 2015 (Act 895) established the Nuclear Regulatory Authority, Ghana in January 2016 as the competent authority for regulation of nuclear and radiological activities in Ghana. The main practices and activities related to radioactive or nuclear material in Ghana are: Medical (General X-ray: computed tomography, mammography, fluoroscopy; Radiotherapy: tele-therapy, brachytherapy, nuclear medicine, linear accelerator [medical]); Industrial (nuclear gauge, oil well logging, destination inspection scanners, industrial radiography); Academic (test sources); Gamma Irradiator Facility; Research Reactor; Linear Accelerator; Radioactive Waste Facility; Borehole Disposal System [BDS]; and ongoing efforts to introduce Nuclear Power Plant by 2029. The Authority has developed Nuclear Security Regulations which comprises provisions for physical protection of nuclear installations, security of nuclear and other radioactive material in use, storage and transport. The regulations also addresses nuclear material accounting and control for nuclear security, nuclear forensics and addresses management systems including institution of nuclear security culture by authorized persons. The regulations address trustworthiness programme of the authorized person as well. The initial effort sought to develop three different sets of regulations for security of radioactive sources, physical protection of nuclear facilities and transport security. The three drafts were developed after which assistance was received from the International Atomic Energy Agency (IAEA) to review the draft regulations. The Authority solicited review of the draft regulations for security of radioactive sources from our various stakeholders including Customs Division of Ghana Revenue Authority, National Disaster Management Organisation, Ministry of the Interior, Attorney General’s Department, Ghana Atomic Energy Commission, Ghana Immigration Service, Petroleum Commission, Ghana Civil Aviation Authority, Ghana Ports and Harbours Authority, Ministry of Environment Science Technology and Innovation as well as international partners such as IAEA and Office of Radiological Security of United States Department of Energy. The transport security regulations and physical protection of nuclear installations regulations have also received review from IAEA Experts after which a National Workshop and Consultative Meeting were held, respectively for the two to consolidate the inputs from the Experts with support from IAEA. A National Workshop is planned to finalise the expert discussion on the Nuclear Security Regulations prior to review by the Nuclear Regulations Guidance Committee of the Authority. Following that review, Stakeholder inputs will be solicited for three months after which a Stakeholder Forum will be held to complete the consolidation of the regulations. The Research and Technical Committee of the Board of NRA will review and forward to the Board for further review. The draft regulation will then be forwarded to the Attorney General’s Department through the Sector Ministry for Parliamentary review and passing as a legislative instrument. It is envisaged that the combination of the entire provisions into a single regulation will meet challenges of defining security levels, setting out general provisions and a tendency to consider the sets as different and only being combined into a single piece. We seek to develop the regulation into a form that will easily be understood and accessible to the authorized person without the tedious effort of blending three different sets of regulations seeking to achieve the similar goal of securing nuclear material and other radioactive materials in use, storage and transport. Ghana’s international cooperation in the development of the regulations is discussed. The active role of the IAEA in the development of the regulations is also presented.
Ghana

**Gender**

Male

**Primary authors:** AMPOMAH-AMOAKO, Emmanuel (Nuclear Regulatory Authority, Ghana); ABOH, Innocent Joy Kwame (Nuclear Regulatory Authority, Ghana); ADU, Simon; APPIAH, kwame (nuclear regulatory authority); AGBENORKU, Obed (Nuclear Regulatory Authority); Mr KYEI, Afrifa Yamoah (Nuclear Regulatory Authority, Ghana); Mr GYAN, Philip (Nuclear Regulatory Authority, Ghana); Mrs MENSAH, Ann Elornam (Nuclear Regulatory Authority, Ghana)

**Presenter:** AMPOMAH-AMOAKO, Emmanuel (Nuclear Regulatory Authority, Ghana)

**Track Classification:** CC: National nuclear security regulations
ROLE OF NUCLEAR SECURITY SUPPORT CENTRE IN DEVELOPMENT OF NUCLEAR SECURITY REGIME IN GHANA

The Nuclear Regulatory Authority Act, 2015 (Act 895) established the Nuclear Regulatory Authority (NRA) to provide for the regulation and management of activities and practices for the peaceful use of nuclear material or energy, radioactive material or radiation; to provide for the protection of persons and the environment against the harmful effects of radiation hazards; to ensure the effective implementation of Ghana’s international obligations and for related matters. The NRA oversees activities of the Nuclear Security Support Centre (NSSC) which provides training support in areas of Nuclear Security, Nuclear Safety and Radiation Protection. The Centre provides equipment support services to front line officers. The NSSC provides assistance in physical protection of nuclear material and nuclear facilities; safeguards, accountancy and control aspects; use of radiation detection equipment by government officials; safety and security associated with radioactive sources; radiation detection equipment and maintenance; combating illicit trafficking of nuclear and radiological materials; search and recovery of orphan sources; nuclear forensics; international legal instruments on nuclear security; wider management skills and development of a nuclear security culture; and awareness raising to policy makers and other public officials whose job requires an appropriate knowledge of nuclear security. There is a need to focus the activities of the Centre to achieve these goals. The Centre has been spearheading training of frontline officers in use of radiation detection equipment and nuclear security. The Centre has hosted fellows of the International Atomic Energy Agency (IAEA) from neighbouring States to assist in developing their knowledge in the use of detection equipment and conduct of nuclear security inspections. This paper provides the discussion on the role of the Nuclear Security Support Centre in developing and sustaining the nuclear security regime in Ghana.

State
Ghana

Gender
Male

Primary authors: AMPOMAH-AMOAKO, Emmanuel (Nuclear Regulatory Authority, Ghana); ABOH, Innocent Joy Kwame (Nuclear Regulatory Authority, Ghana); ADU, Simon; MENSAH, Ann (Nuclear Regulatory Authority)

Presenter: AMPOMAH-AMOAKO, Emmanuel (Nuclear Regulatory Authority, Ghana)

Track Classification: CC: Role of Nuclear Security Support Centers to support and sustain national nuclear security regimes
NUCLEAR SECURITY INFRASTRUCTURE FOR DISPOSAL OF DISUSE SEALED SOURCE IN A BOREHOLE

The potential consequences of an act of terrorism using radioactive sources can be gauged from the consequences of serious accidents that have occurred involving radioactive sources. These include fatal and injurious radiation exposures, contamination of the environment, and serious economic and psychosocial costs the total effect of which is mass disruption. Steps are being taken to improve security for radioactive sources but strategic approaches that can minimize the threat of radiological terrorism should be considered. When justifying a practice that uses radioactive sources, the potential for diversion or use in terrorism should be considered to be a detriment. In this regard, the consideration and development of alternatives to radioactive sources, such as radiation producing machines, have been recommended by terrorism experts as measures to reduce the threat of radiological terrorism. If a practice using radioactive sources is determined to be justified, the need for special security measures to protect against terrorism should then become part of the safety assessment. After the 9/11 attack on the US there has been an increase in awareness of threat associated with disused radioactive sources around the globe. Attention had been drawn to the fact that there should be an increase awareness of the need for safety and security measures to protect against the potential use of radiation sources in terrorism. The first Nuclear Security Summit held in Washington in April 2010 focused mainly on the security of weapons-grade nuclear material such as highly enriched uranium (HEU) and separated plutonium but some leaders highlighted on the need of also securing other radioactive material, especially radioactive sources and urged participants to adequately address the risks associated with their use. These risks comprise – accidents following loss of control over, improper use or disposal of radioactive sources (disused and orphan sources), – malevolent use ranging from theft over illicit trafficking to the potential misuse by terrorists through building so-called dirty bombs.

The over six decades of peaceful application of Sealed Radioactive Sources (SRS) have resulted in the generation of Disused Sealed Radioactive Sources (DSRS) in Ghana. They represent a significant security threat and safety concerns to human health and the environment. They therefore must be managed in a safe and secure manner to reduce threat of getting to the hand of an adversary. The Radioactive Waste Management Centre (RWMC) established by Ghana Atomic Energy Commission (GAEC) was tasked to carry out the safe and secure management of radioactive waste materials generated at GAEC and in Ghana as a whole. The RWMC operates a secured Centralised Radioactive Waste Storage facility for characterization and storage of radioactive waste materials. Storage is an important interim management step, especially for DSRS containing very short-lived radionuclides, which can decay to exemption levels within a few years. However, long-term storage is considered unsustainable option for DSRS with long half-lives radionuclides such as Ra-226, which has a half-life of 1600 years.

A national policy and strategy on the management of these disused sources is part of a broader policy and strategy, which will enable the Ghana to address all these provisions relating to management of disused sources in a comprehensible manner. The IAEA Guidance on the Management of Disused Radioactive Sources recommends States to incorporate provisions for the safe and secure management of disused sources into their legislation and regulations. The implementation of security measures for radioactive sources must take into consideration the potential for deliberate acts to attack or use radioactive sources to expose people and cause contamination. The IAEA NSNS has over the years worked with Members States to securely manage Category 1 and 2 disused
sources, through assessment missions, repatriation of disused sources, export of disused sources for recycling, and the pilot borehole disposal project. As Ghana does not have an extensive nuclear power programme that would require the development of a deep geological disposal facility, the GAEC have proposed the International Atomic Energy Agency’s (IAEA’s) developed Borehole disposal Of Spent Sources (BOSS) system for management of the DSRSs. The Government of Canada, support from the U.S. Nuclear Regulatory Commission’s (NRC’s) and the International Atomic Energy Agency (IAEA) is supporting the field deployment of the Borehole Disposal Concept (BDC) in Ghana, the Philippines and Malaysia for secure disposal of radioactive sources in Ghana. This is a first-of-its-kind implementation. The paper is to look at the nuclear security Infrastructure for disposal of disuse sealed source in a borehole in Ghana. It will highlight the national regulatory framework for managing DSRS in Ghana.

**State**

Ghana

**Gender**

Male

**Primary authors:** ADU, Simon; GLOVER, Eric Tetteh (Ghana Atomic Energy Commission); AM-POMAH-AMOAKO, Emmanuel (Nuclear Regulatory Authority, Ghana); Prof. FAANU, Augustine (Graduate School of Nuclear and Allied Science, University of Ghana-Atomic Campus); ABOH, Innocent Joy Kwame (Nuclear Regulatory Authorithy, Ghana)

**Presenter:** ADU, Simon

**Track Classification:** CC: Innovative technologies to reduce nuclear security risks and improve cost effectiveness, where feasible
As the number of cancer cases and deaths in Africa continues to rise, African states are racing to get ahead of this wave by acquiring additional radiotherapy machines. In doing so, these countries not only face financial challenges, but considerations of whether to use linear accelerators, which both offer better cancer care and reduce radiological security risks, or cobalt-60 machines, which are inferior on both counts, but often cost less and operate more consistently in more challenging environments.

To be sure, the trend line is clear: better-off African countries, such as South Africa and Nigeria, have moved almost entirely to LINAC based treatment. This shift can be attributed not only to the superior performance of these machines, but rising terrorist attacks and threats in Africa, enhancing radiological security concerns. Nonetheless, more than eighteen African countries still have co-60 machines, while thirty-nine generally poorer African countries lack a single teletherapy machine and may consider purchasing additional co-60 machines.

There currently are hundreds of thousand cancer-related deaths each year in Africa, projections indicate that could rise to a 1.4 million new cancer cases and 1 million cancer deaths in Africa annually by 2030. In light of the increasing terrorist threat, it is becoming extremely difficult to ignore the serious security threat that would be created by countries that plan to address the current shortfall of more than 4000 radiotherapy machines by establishing or upgrading radiotherapy facilities with high-risk cobalt-60 units. The specific current and future radiation therapy equipment needs met by high-activity radioactive sources may over time selectively be met by alternative technologies based on lower activity sources or no radioactive sealed sources at all.

Many governments and organizations in Africa have undertaken initiatives to facilitate the adoption and sustained use of security risk-free LINAC-based radiotherapy machines. Many of the research studies conducted to date on the cobalt-to-linac transition in Africa have been descriptive in nature addressing obstacles and making recommendations, but not instructive. The aim of this paper is to critically describe the transition process and lessons learned from the African experience and perspective. The research data analyzed in this study are drawn from four main sources: the IAEA Directory of Radiotherapy Centres, the Federation of African Medical Physics Organizations, Elekta and Varian (two manufacturers). Our findings have significant implications regarding the impact of introducing alternative radiotherapy technologies to enhance the “treatment” and reduce the “terror” in the treatment not terror paradigm.

**State**

Cameroon

**Gender**

Male

**Primary authors:** Mr FOY, Hubert (African Centre for Science and International Security); ZU-BIZARRETA, Eduardo (Section Head ARBR - NAHU - IAEA); POMPER, Miles (James Martin Center for
Nonproliferation Studies; COLEMAN, C. Norman (International Cancer Expert Corps); Dr DALNOK-I-VERESS, Ferenc (James Martin Center for Nonproliferation Studies)

**Presenter:** Mr FOY, Hubert (African Centre for Science and International Security)

**Session Classification:** Innovative technologies to reduce nuclear security risks and improve cost effectiveness, where feasible

**Track Classification:** CC: Innovative technologies to reduce nuclear security risks and improve cost effectiveness, where feasible
SECURITY OVERSIGHT OF CONVERSION OF GHANA RESEARCH REACTOR-1 FROM HIGH ENRICHED URANIUM TO LOW ENRICHED URANIUM FUEL

In line with the global efforts at reducing and eventually eliminating the civilian use of High Enriched Uranium as fuel for reactor cores, Ghana has successfully undertaken the conversion of the Miniature Neutron Source Reactor core to Low Enriched Uranium, at the Ghana Atomic Energy Commission, and returned the spent fuel to China. The nuclear security aspect of the regulatory oversight of this event was under the auspices of the Nuclear Security Committee of Ghana which is coordinated by the National Security Council Secretariat and chaired by the Director General of the Nuclear Regulatory Authority. The submittals received and the review conducted led to involvement of the Nuclear Security Committee which assisted with the conduct of Scoping Missions, Dry Run, issuing of Administrative Instructions and provision of security cover for the conversion. The roles played by various organizations forming part of the Nuclear Security Committee in securing the transport of the used fuel are discussed along with experiences obtained. The assistance received from the International Atomic Energy Agency and the support of the United States Government are also presented along with lessons learnt.

State
Ghana

Gender
Male

Primary authors: AMPOMAH-AMOAKO, Emmanuel (Nuclear Regulatory Authority, Ghana); ADU, Simon; MENSAH, Ann (Nuclear Regulatory Authority); EMI-REYNOLDS, Geoffrey (Ghana Atomic Energy Commission); Mr BAFFOE-MENSAH, William (National Security Council Secretariat)

Presenter: AMPOMAH-AMOAKO, Emmanuel (Nuclear Regulatory Authority, Ghana)

Track Classification: PP: Research reactor security
A process data integrated dynamic cybersecurity risk assessment approach for industrial control system

As digital instrumentation and control (I&C) systems are more fully integrated into nuclear power plants (NPPs) and communication networks cross boundaries of the business and operational systems, new opportunities for disrupting NPP operations are introduced. Enhancing the cybersecurity of digital I&C systems is key to ensuring the safety and economics of the nuclear power industry. Dynamic cybersecurity risk assessment helps decision-making by updating the risk value with architecture or configuration changes and cyber-attack movements.

The cybersecurity risk should include malicious cyber-attacks and unintentional cyber-incidents resulting from human factors. Here, the term cyber-events is used to indicate these two. Cybersecurity risk assessment starts with vulnerability analysis for every digital device in the system. Common vulnerability libraries such as Common Vulnerabilities and Exposures (CVE) are used for finding entry points and vulnerabilities in these devices. To assess the risk accurately, ideally IT experts should find all possible attack paths for a system. However, it is impossible to emulate all the possibilities. Therefore, unknown cyber-attacks, such as zero-day attacks as well as unintentional cyber-incidents will lead to underestimation of the risk if they are excluded. One possible way of reducing these unknown factors is integration of process data into the evaluation of cybersecurity risk. An unsupervised anomaly detection model, which detects deviation from normal operation using process data results from cyber-events, is built to perform continuous risk assessment by updating the detected abnormal behavior. In addition, To avoid risk overestimation caused by process data deviation from a safety event, such as equipment and system failure or degradation, a model is proposed to distinguish cyber-events and safety events with a confidence interval.

Current literature suggests that the Bayesian network is a widely used approach in cybersecurity risk assessment because it conveys intuitive causal information as well as the conditional probabilities. Bayesian network is a directed acyclic graph (DAG) which is composed with nodes as variables and directed arcs which represents the conditional dependencies. The probability distribution of the nodes are usually presented by a conditional probability table (CPT).

A comprehensive dynamic cybersecurity risk assessment architecture is proposed in this research which consists of an evidence collection module which gathers information to identify the evidence of a cyber-event, including distinguishing the cyber-event and safety event; a Bayesian Network which presents intuitive dependency of different events; a regularly updated CPT built by Information Communication Technology (ICT), Operational Technology (OT), and Cybersecurity experts; and a risk value generation module which updates the risk dynamically.

A case study based on a real-time industrial control system (ICS) test bed will be conducted to demonstrate the proposed approach. This test bed consists of a physical experiment facility which simulates a typical two-loop nuclear power system thermal hydraulic component and a Supervisory Control and Data Acquisition (SCADA) system which controls the facility. A Bayesian Network will be built with a node description table. Simulated attacks will be conducted to assess the dynamic behavior of the proposed approach.

State

United States

Gender
Female

**Primary authors:** Ms ZHANG, Fan (University of Tennessee-Knoxville); Mr SPIRITO, Christopher (Idaho National Laboratory); Prof. COBLE, Jamie (University of Tennessee-Knoxville)

**Presenter:** Ms ZHANG, Fan (University of Tennessee-Knoxville)

**Track Classification:** CC: Information and computer security considerations for nuclear security
Cybersecurity in Research Centers: Focus on nuclear and radioactive facilities.

Cybersecurity in Research Centers: Focus on nuclear and radioactive facilities.

The Cybersecurity Research Center’s standards for handling nuclear and radioactive materials should be built on a "defense in depth" model. This model should be suitable for the existing ecosystem and should consider all cyberthreats that can and undermine existing security, with the objective of compromising critical telecommunications infrastructure, information systems, nuclear control systems, and radioactive data research centers, eliminating and exposing sensitive data.

Cybersecurity in a nuclear and radioactive facility should focus on an in-depth defense model. Protective barriers or defenses should delay cyberattacks and complement the protection of critical infrastructures involving the control and management of nuclear and radioactive components, as well as the physics of administrative and security systems.

In order to develop in depth the defence model to protect the information and industrial control systems of nuclear and radioactive facilities, each of the layers of the proposed model must be analysed, giving the real value corresponding to each of the critical or vital assets, including each of the risks that may infringe the defined defence layers.

The defense model proposed in depth must be in a cycle of continuous improvement through planning, implementation, review and improvement actions. These actions aim to evaluate the original plan, add new critical infrastructures that have been identified, add new threats and registered security incidents.

The concept of in-depth defence applied to the field of nuclear safety comes from the latest "Three Mile Island" accident works. It is defined as a defence that includes three successive independent barriers that lead to an extremely low level of probability that an accident may have an off-site impact. The idea is that each safety device must be considered a priori as vulnerable and therefore must be protected by another device.

In order to establish a defence model in depth, the following definitions are proposed:
- The severity of a given value measures the real impact of the incident based on the criticality of the asset or the potential impact of the incident on the threatened fine.
- A measurement scale is proposed that establishes the levels of severity, with the objective of comparing the different security incidents generated by the impact. Users are responsible for determining the appropriate level of seriousness to be appreciated in light of the impact of the incident on the asset to be protected.
- A barrier is a security means capable of protecting a part of the information system against at least one threat. A barrier can be human, a method can be static or dynamic, and manual or automatic. It must have a means of control that shows the state of operation of the barrier.

- A line of defense is a set of barriers, and the overcoming causes an incident whose severity depends on the number of barriers still to be overcome by the threat or threats, in order to achieve a property or protected property.
- The defense in depth of information systems is a global and dynamic defense that coordinates several lines of defense to cover all the depth of the system.

State

Mexico
Gender

Male

Primary author:  Mr PEREZ, Juan Manuel (National Institute for Nuclear Research)
Presenter:  Mr PEREZ, Juan Manuel (National Institute for Nuclear Research)

Track Classification:  CC: Information and computer security considerations for nuclear security
Cyber Security Administrative and Technical Control Measures for Reducing Insider Threats

Cyber security defense strategies to detect, counter and respond to cyber attacks become increasingly challenging when the threats originate from within, from the organization’s authorized users. The term “insider threat” is often used to describe members of an organization, or associates such as a contractor, with malicious intent. However, threats can also result inadvertently from employees, or from policy violations which allow malicious outsiders to gain system access.

An increasing number of threat cases, from high profile data leaks to even the most successful external attacks, have some insider threat component. This illustrates the importance of developing an insider threat program. This paper seeks to identify best practices to mitigate or reduce insider threats, whether intentional or inadvertent, using administrative and technical controls.

State

Jamaica

Gender

Male

Primary author:  Mr THOMAS, Mckeane (International Centre for Environmental & Nuclear Sciences (ICENS))

Presenter:  Mr THOMAS, Mckeane (International Centre for Environmental & Nuclear Sciences (ICENS))

Track Classification:  CC: Information and computer security considerations for nuclear security
The Past and Potential Role of Civil Society in Nuclear Security

While the operators managing nuclear facilities and materials play the most critical roles in implementing nuclear security day-to-day, civil society has played a very important role in nuclear security over the years, and its role could be strengthened in the future.

Some nuclear organizations react against the very idea of civil society involvement, thinking of only one civil society role – protesting. In fact, however, civil society has played quite a number of critical roles in nuclear security over the years. Some of these roles have included:

• **Highlighting the dangers of nuclear terrorism.** Ever since John McPhee’s seminal The Curve of Binding Energy in 1973, civil society experts have been central to calling attention to the dangers nuclear security systems are designed to protect against, helping to motivate governments to act.
• **Suggesting actions to be taken.** Here, too, civil society experts have played prominent roles for many years. As the Soviet Union neared collapse, Ashton Carter, then a professor at the Harvard Kennedy School, helped draft the Nunn-Lugar legislation on U.S.-Russian cooperation to secure and dismantle the excess weapons of the Cold War. Later, one of the authors (Bunn) first suggested the four-year effort to secure nuclear material around the world that was the key commitment agreed to at the first Nuclear Security Summit in 2010. Many operators around the world have implemented suggestions from the good practice guides of the World Institute for Nuclear Security (WINS), contributing to nuclear security improvements around the world.
• **Nudging governments to act.** Civil society actors have often gone beyond making suggestions to more active efforts to promote government action. In the early 2000s, for example, the effort to launch a program to remove weapons-usable nuclear material from potentially vulnerable sites included analysis, work to draft legislation, and the Nuclear Threat Initiative (NTI) stepping in and providing the funds needed to get a deal to remove highly enriched uranium (HEU) from what is now Serbia. Those ultimately led to the launch of the Global Threat Reduction Initiative – and today, more than half of the countries that once had separated plutonium or HEU on their soil have gotten rid of it. Just before the September 11, 2001 attacks in the United States, one of the authors (Bunn) developed a proposal for NTI to give the IAEA a gift to support its physical protection work; after the attacks, that NTI gift and a matching grant from the U.S. government were the founding gifts of what is now the Nuclear Security Fund. Civil society efforts to track whether governments were living up to their commitments from the nuclear security summits have helped hold governments accountable for their pledges.
• **Educating the public and other players.** From universities to think tanks, civil society actors play a particularly important role in education – as reflected by the large number of them participating in the International Nuclear Security Education Network (INSEN). This includes not just educating the general public, but educating legislators and other government officials, and even nuclear security operators as well. Today, the WINS Academy is playing a particularly prominent role, providing education and professional certification for hundreds of nuclear security professionals in dozens of countries.
• **Promoting dialogue and partnerships.** A key civil society role which underlies many of the others is their role in promoting dialogue and encouraging partnerships and cooperation among other actors. While there are countless examples, NTI’s Global Dialogue is a particularly prominent one, bringing together government officials, industry experts, and civil society experts to discuss key issues and ideas in a more informal and creative way than would ever be possible in government-to-government negotiations.
In short, civil society has played a key role in nuclear security in the past and is likely to continue to do so in the future. Funding organizations (both government and non-government) should consider ways to support civil society work and expertise focused on nuclear security in additional countries. Rather than simply protesting and opposing, civil society can help lead to more effective nuclear security practices around the world.

State

United States

Gender

Male

Primary authors:  BUNN, Matthew (Harvard University); ROTH, Nickolas (Belfer Center, Harvard University)

Presenter:  BUNN, Matthew (Harvard University)

Track Classification:  CC: Implementation of national legislative and regulatory frameworks, and international instruments
The Need for Creative and Effective Nuclear Security Vulnerability Assessment and Testing

Realistic, creative vulnerability assessment and testing is critical to finding and fixing nuclear security weaknesses and avoiding over-confidence. In the U.S. experience, nuclear security systems that looked great on paper have often failed, in evaluations or tests, to protect against mock adversaries who had found a clever approach to defeating the defenders.

Both vulnerability assessment and realistic testing are needed to ensure that nuclear security systems are providing the level of protection required. A checklist approach that simply asks whether the system has all the particular elements required by regulations is not sufficient. Instead, systems must be challenged by experts thinking like adversaries, trying to find ways to overcome them.

Vulnerability assessment can make use of a variety of tools and approaches, from examination of individual security elements to find ways they might be defeated to complex computer simulation software modeling possible adversary efforts to defeat the system. Perhaps the most important element is the creativity and adversary mindset of the assessors; they should be genuinely looking for weak points, not just seeing whether the system will protect against a few pre-programmed attack strategies.

Nuclear security testing is closely related. Testing can provide data for use in vulnerability assessments and can help check the validity of assumptions and plausibility of proposed tactics. The results of realistic testing are often more convincing to organizational leaders and policymakers than any amount of paper or computer analysis. Testing can range from testing the performance of particular pieces of equipment to testing of the site’s full security system in a force-on-force exercise. Here, too, it is key to ensure that testers are creative and thinking like adversaries, imagining and testing clever ways adversaries might attempt to defeat the security system.

Both effective vulnerability assessment and realistic testing are more difficult in the case of insider threats. Much of the software that has been developed for vulnerability assessment simulation is stronger for outsider threats than for insider threats, and finding realistic ways to test insiders’ ability to exploit their trusted access to conduct adversary actions without compromising safety and security is difficult. A variety of approaches have been developed, however, and further development is ongoing.

Ensuring such creativity becomes an issue of organizational security culture, as some organizations tend to react against assessors and testers who regularly find weaknesses in the security system, rather than rewarding them. Organizations need to find ways to give people the mission and the incentives to find nuclear security weaknesses and suggest ways they might be fixed. But with the right approaches and incentives in place, effective vulnerability assessment and testing can be a key part of achieving and sustaining high levels of nuclear security.

State
United States

Gender
Male
Primary authors: BUNN, Matthew (Harvard University); ROTH, Nickolas (Belfer Center, Harvard University)

Presenter: ROTH, Nickolas (Belfer Center, Harvard University)

Track Classification: PP: Nuclear security vulnerability assessments
REGIONAL INFORMATION SHARING SYSTEM TO COMBATE NUCLEAR TERRORISM A PROBABILISTIC RISK ASSESSMENT APPROACH

The probabilistic risk assessment (PRA) methodology qualitatively can be applied as a most practical tool to address the problem of nuclear terrorism and efforts to reduce risk in the region of concern where roots of smuggling can be traced by constructing event trees. PRA can also be used as a tool for mitigating the consequences in case of occurrence of an unwanted attack.

The problem we have to address is:

i. How to assess the risk of nuclear terrorism

ii. How to prevent the risk of illicit trafficking of radioactive materials

iii. How to reduce the nuclear risk with regional cooperation efforts.

Radioactive and nuclear materials smuggled for illegal use can always cause a threat to human health and environmental safety whether they are discovered (seized) or may never be discovered. In this paper, it is proposed that the probabilistic risk assessment methodology in detecting and preventing terrorist attacks can be used to determine the accident sequences that lead to system failures, to remove weak links of the system, and also to help those who regulate the shipping and port establishments.

In order to make a qualitative and if possible quantitative risk assessment to the problem of the misuse of nuclear or radioactive material for producing of nuclear arms, explosives, use in terrorist attacks, questions to be addressed and actions to be taken for probabilistic logic approach may be as followings:

• Why illicit trafficking or smuggling? Analyze reasons and list initiating events
• What type of nuclear materials was smuggled in the past? Risks involved?
• Where would they go and they are handled? Work on event trees. Try to construct event trees on several scenarios
• What are the probabilities involved. Try to quantify probability of occurrence and select most probable event trees
• What might be the consequences?
• What could happen if serious nuclear attack occurs? Prepare emergency plans
• How the end results can be mitigated
• What are the lessons learnt? and

The one of the most important question which comes last but it should be the first:

• Who will be most affected hence should be more concerned? Classify groups such as

  International concern
  Regional concern
  National governmental concern
  Local governmental concern
  Public concern

and analyze whether or not these groups have sufficient awareness and identify key groups to be addressed for a new initiative of a security awareness programs and to be supplied with more information to increase the awareness.

State

Turkey
Gender
Female

Primary author:  Ms GÖKTEPE, Bahire (NUTEK Energy)
Presenter:  Ms GÖKTEPE, Bahire (NUTEK Energy)

Track Classification:  MORC: Preventing illicit trafficking of nuclear and radioactive material
Results of the EU project for an effective Container Inspection at Border Control Points (C-BORD) in Support to Customs

An efficient non-intrusive inspection (NII) of containerised freight is critical for customs, as freight containers are potential means of smuggling, illegal immigration or even trafficking nuclear material and chemical warfare agents. Thousands of freight containers and trucks pass every day at any small to medium port or border within the EU which potentially makes them an ideal means for the illicit transport and trafficking of radioactive and nuclear materials (including waste and contaminated commodities) as well as for the smuggling of drugs and narcotics, tobacco, weapons, explosives, chemical warfare and humans. This creates many challenges for customs and border control authorities who must ensure that adequate inspection means and solutions are in place for an optimum interdiction chain that is safe, practical, and cost-effective and on the other hand remain non-intrusive in order to facilitate trade on one hand and ensure safety and security of the society.

Thus an efficient non-intrusive inspection (NII) of containerised freight is increasingly important to trade and society, as the criminal disruption of supply chains can severely harm the economy, as well as endanger public health and safety. The current methods for container NII combine intelligence-supported risk analysis and X-ray technology to combat illicit trafficking. However, this approach is limited due to health and safety regulations, long operator processing time to manually check containers in case of a doubt and a lack of reliability due to insufficient ability to distinguish between innocent items and threats.

The objectives of C-BORD was to enable customs to deploy comprehensive and cost-effective solutions for the NII of containers in order to protect the European Union sea and land borders. To that effect and following the success of earlier EU projects such as SCINTILLA, the Effective Container Inspection at Border Control Point (C-BORD) project was launched in June 2005, funded (11.8 M€) within the EU H2020 programme to support a consortium of eighteen partners (industry, universities, research centres, users) and from nine EU member states not only to develop but also integrate five detections and inspection technologies. The technologies selected and pursued namely the next generation cargo X ray, tagged neutron interrogation, evaporation (or sniffer), advanced radiation portal monitors and photo fission were tested in laboratories such as at the JRC-Ispra, CEA (France) and EK (Hungary) followed by extensive field testing (on targeted use cases) prior to closure of the project by a well-attended public workshop which included a demonstration at the Rotterdam harbour. Most importantly and for the first time, the data generated by the five technologies were collated very conveniently in a single graphic user interface to simplify, speed up and an effective and correct customs decision-making.

This paper will describe the project, its structure and the technologies developed and integrated and will give its main results and conclusions.
Primary authors:  Mr SANNIE, Guillaume (CEA-LIST); Dr TAGZIRIA, Hamid (European Commission, Nuclear Safety and Security Directorate, Nuclear Security Unit); Mr PILORGET, Benoit (ART-TIC)

Presenter:  Mr SANNIE, Guillaume (CEA-LIST)

Track Classification:  MORC: Preventing illicit trafficking of nuclear and radioactive material
CHALLENGES IN IMPLEMENTING NUCLEAR SECURITY SYSTEMS AND MEASURES IN MAJOR PUBLIC EVENTS IN UGANDA

The nuclear law for regulation of peaceful applications of radioactive sources in Uganda was enacted in 2008. The law established the Atomic Energy Council as the national regulatory body in the nuclear energy subsector. The Act also provided for radiation safety, radiation protection and nuclear security in the applications of radioactive sources in the country.

The increasing use of radioactive materials in the medical, industrial as well as research and education sectors, though, has numerous benefits, it is associated potential risks. The increasing importation of radioactive sources by the different operators in the various sectors of development in Uganda point to the increasing number of radioactive sources in the public domain. Although the Act provides that the responsibility for radiation safety and nuclear security is primarily on the authorised persons, there have been incidences in Uganda where radioactive sources get out of regulatory control. These radioactive sources if not managed safely and securely protected, pose high risk to human health and the environment. The risk posed by these materials is amplified when they end up in the hands of the unauthorised persons who could use them for malicious acts to satisfy their selfish interests.

The potential of the risk would even have worse consequences when used against people gathered in large numbers particularly on major public events. Uganda on annual basis and in some cases, on particular occasions holds such events. One of such events is when the Uganda government hosted the Pope in 2014 which attracted over two million people in one place. Other such events include Uganda Martyrs day, Independence anniversary celebrations, presidential sharing for new president and some presidential election campaign events among others.

During major public events, the national security agencies draw up general security plans for such events. However, times and again, nuclear security had not been given the due consideration and on many occasions not incorporated in the general security plans. Nevertheless, during the preparations for the pope’s visit to Uganda, the Atomic Energy Council proposed the inclusion and implementation of nuclear security measures and systems in the general security plan for this major public event. This was adopted by the security agencies during the Pope’s visit and many other subsequent major public events.

The IAEA supported nuclear security preparations through training of security personnel (FLO, Bomb squad) and the personnel from the regulatory body (MEST) as well as loaning equipment to be used during the event and to be returned after the event. Although the event went on well without any nuclear incidents or accidents, this was not without challenges that affected the proper implementation of nuclear security measures and systems, such challenges as lack of awareness, concepts of operations, lack of competent and experienced personnel(MEST) and the lack of equipment among others factored themselves in the implementation strategies that were adopted.

This paper will highlight the challenges encountered in the implementation of nuclear security systems and measures as well as the lessons learned in implementing nuclear security measures and systems for major public events in Uganda.

State

Uganda
Gender
Male

Primary author: LUWALIRA, Noah Deoh (Atomic Energy Council)
Presenter: LUWALIRA, Noah Deoh (Atomic Energy Council)

Track Classification: MORC: Nuclear security as part of the security of major public events
IMPROVED SPECIFICATIONS, PERFORMANCE, AND UNDERSTANDING OF RADIATION DETECTION EQUIPMENT USED FOR NUCLEAR SECURITY – OUTCOMES OF PARTICIPATION IN IAEA COORDINATED RESEARCH ACTIVITIES

The Coordinated Research Project (CRP) J02012 has been deployed by the IAEA in the theme of "Advancing Radiation Detection Equipment for Detecting Nuclear and Other Radioactive Material out of Regulatory Control". The objective of the CRP was to determine and fulfill the gaps between nuclear security (NS) needs and existing capabilities of the detection instruments. The final goal of the project was to assure the sustainability of the nuclear security regime on a local and global scale. Sri Lanka, as one of the participating Member States in the CRP, has received tremendous benefits through it.

Sri Lanka’s major improvements and achievements on its NS regime through the CRP can be identified in both technical and managerial context. Sri Lanka Atomic Energy Board (SLAEB) has been a part of the CRP from 2017 and received assistance for the development, improvement, and sustainment of NS detection. The paper discusses these improvements as fruits of the project and encourages other Member States to collaborate in CRPs.

The technical gain from CRP can be expressed further using the significant improvements in a) instrument selection and in b) detection capabilities. The understanding of the identification of suitable instruments and specifications has been enhanced with the assistance of the CRP. This can be further explained in the scopes mentioned in figure 01. The detection capabilities were tested and identified gaps have been reduced through networking & combination of instruments, improving the performance and developing the ways of assuring technical sustainability.

The managerial gain from CRP can be explained in a) improvement of approach and b) sharing of knowledge and experience. This intangible development was primarily facilitated by sharing of experience and by inter-state, inter-organization collaborations. The approach to the NS has been expanded through the exposure to international and institutional NS cultures. Also, the CRP has developed a platform to establish links among the stakeholder member states. With this improved approach, the members have been strengthened up through sharing of the knowledge, experiences on best practices, ways of overcoming challenges and understanding limitations of detection instruments.

The needs of the NS stakeholders have been identified through a systematic need analysis performed using a sample of Front-line Officers (FLOs) and expert competent authorities working in NS. This response can be considered as a critical input to understand the instrument characteristics valued by the field officers and the performance required by the competent authorities and its experts. Apart from that, tests for assessing the performance of the NS detection instruments are being conducted by the SLAEB’s instrument research team to fulfill the objectives of the CRP J02012. The results obtained through these descriptive studies are also presented by this document.

State

Sri Lanka

Gender

May 9, 2020
Primary authors: Mr RANASINGHE, Ranasinghe Arachchige Nirodha Chaturanga (Radiation Protection & Technical Services Division); Mr MAHAKUMARA, Prasad Dhananjaya (Radiation Protection & Technical Services Division, Sri Lanka Atomic Energy Board); Ms RATHNAWEERA, Patabedige Nirasha Gayani (Radiation Protection & Technical Services Division, Sri Lanka Atomic Energy Board); Mr KARIYAWASAM, Kapu Kankanamage Buddhika (Radiation Protection & Technical Services Division); Dr MASSEY, Charles (Division of Nuclear Safety and Security, International Atomic Energy Agency); Ms CHAIRAM, Issaria (Division of Nuclear Safety and Security, International Atomic Energy Agency)

Presenter: Mr RANASINGHE, Ranasinghe Arachchige Nirodha Chaturanga (Radiation Protection & Technical Services Division)

Track Classification: MORC: Detection technology development and performance testing
Blue team support for EPS related cybersecurity readiness

In the context of penetration testing a Red Team of highly skilled IT security experts challenges the security posture of an IT infrastructure within an agreed upon perimeter. They are countered by a Blue Team. The Blue Team identifies possible vulnerabilities and enforces the network security and the security of all digital devices. While the Red Team performs a cyberattack, the aim of the Blue Team is to provide strong defense against the ongoing cyberattack by improving and applying defense mechanisms. The Blue Team focuses on risk intelligence and data analyses, Distributed Denial of Service (DDoS) testing, log and memory analyses, etc. In this paper, we are focusing on Blue Team support and readiness for Electrical Power System (EPS) by providing suitable tools and methods to detect cyberattacks. Accordingly the Blue Team focus is not limited to an understanding of the IT, but comprises the target domain specific knowledge (NPP, EPS and I&C).

In the context of this paper, the main task for a Blue Team is to identify potential threat scenarios. This identification is done by observing a designated Simulink Model for the EPS of a nuclear power plant (NPP) and leads to knowledge about potential future attacks and the means to mitigate these by using suitable tools.

Electrical power systems of a NPP are important not only for electricity generation and power supply to the house load but also essential to the safety and normal operation of a plant. Due to the rising degree of digitization within NPP, electrical protection devices have become more and more digitized. Hence, a cyber-attack could lead to a failure of one of the main electrical systems (e.g., electrical generator or circuit breaker) and can impact the operation of a NPP. A cyberattack could also cause malfunctions of primary or secondary cooling pumps in NPP by attacking the protection devices which are protecting the electric motor of the pump, in order to damage it. Therefore, electrical power systems inside a NPP should also be considered for cybersecurity related analyses.

Within the scope of the IAEA CRP J02008 project, we have modeled a simplified version of the EPS of a hypothetical nuclear facility called ‘Asherah’. The model is implemented by using Matlab Simulink to provide a simulation base for cybersecurity related tests. The Simulink model encompasses mainly electrical systems inside a nuclear power plant. Main components involved in power generation, power supply to the main grid and to the house load, such as electrical generator, generator circuit breaker, auxiliary transformer and some cooling pumps as house load, are covered by the Simulink model.

In research work, we are connecting our Matlab Simulink model with a real piece of hardware (electrical protection relay, programmable logical controller, operating panel, etc.) to simulate the impact of a cyberattack on an electrical system (for e.g., an electrical motor driving a Feed Water Pump).

The Physical access to the components is also within the scope of the attack detection and evaluation process of the Blue Team. Electrical cabinets containing electrical protection devices (e.g., relays) and other electrical devices are placed in a room which is protected by physical access control. During maintenance or normal operation, an attacker could gain access with mischievous intention to these rooms where EPS digital devices are placed by violating physical access control. This could be achieved by stealing a person’s ID to enter into the room and by cracking the password, by maintenance staff with access permission to the room combined with the use of infected software or privilege escalation etc.
For the test, we assume that the potential attacker has background knowledge of digital electrical devices. Cyberattacks (for e.g., Denial of Service, Man in the Middle attack, etc.) will be performed on the real hardware and network data and host data would be collected using different tools (for e.g., Wireshark) and later on anomaly detection would be performed as part of the Blue Team support to electrical systems to withstand against cyberattacks in future.

Beyond the integration of the interface of the EPS model with the real digital devices, a key benefit for the Blue Team is the exercising and training of “what if” scenarios. These can be simulated in the model and the model computes and shows what the impact at the overall EPS and NPP level will be. For these preparations the understanding (and mitigation) of the impact of an attack is essential, without regard on how the Red Team achieved the exploitation of a vulnerability at the IT and I&C level.

**State**

Germany

**Gender**

**Primary author:** Ms GUPTA, Deeksha (PhD Candidate)

**Co-authors:** Ms GOVINDARAJ, Dharini; Dr WAEDT, Karl; ALTSCHAFFEL, Robert (Otto-von-Guericke Universität Magdeburg)

**Presenter:** Ms GUPTA, Deeksha (PhD Candidate)

**Track Classification:** CC: Information and computer security considerations for nuclear security
**Nuclear Security Supporting And Enabling The Peaceful Use Of Nuclear Power – Portability Of Competent Authority’s Assessment Activity To Third Party States**

Small Modular Reactors (SMRs) and other Advanced Nuclear Technologies (ANTSs) offer potential advantages in respect of being quickly deployable and requiring lower capital investments. However, in respect of security, what benefit can a competent authority (CA) take from another CA’s assessment of security (including security by design - passively engineered) in a reactor technology, especially modularised technology? If a CA can take no benefit then, as a community of CAs, we risk inflating the price of and delaying installation of the next generation of potentially simpler, quicker and cheaper to install, nuclear power.

It is not the CA’s role to promote nuclear power but can the CA community remove barriers by working together? Naturally there will be differences in DBT so the importing CA will of course want to do some form of assessment but this paper suggests it need not start with a blank page.

Through CPPNM compliance CAs already accept foreign flagged vessels in territorial waters so there is a precedent, albeit tenuous, of taking account of other CAs’ security regimes in an international context. Many states already import reactor designs from other states. Does the importing CA start from a zero base assessment of the security characteristics and required physical protection or does it take account of the assessment activity of the exporting CA? If so to what extent?

The UK has a mature process for assessing reactor designs before construction, seeking to ensure safety and security by design and decreasing risks of construction, known as generic design assessment (GDA). The UK GDA process, which for security purposes is described in the Security Assessment Principles (SyAPs), Technical Assessment Guides (TAGs) and other regulatory guidance published on ONR website. UK GDA includes a comprehensive security assessment, specifically security by design, taking account of all conceptual security arrangements, from leadership and management for security, organisational culture, competence, EMIT, supply chain, physical measures for theft and sabotage, computer security including operational technology, workforce trustworthiness, emergency response and policing and guarding. The regulatory guidance against which the assessments are undertaken is largely published, with the exception of a limited number of classified annexes and one of 37 TAGs, hence an importing CA can clearly understand the nature of assessment that would be undertaken by the UK CA and target its own supplementary assessment, if required, at areas it considers appropriate.

Naturally no two states will have the same DBT and states are unlikely to share their DBTs with other states. Therefore an importing CA may ask whether an exporting CA’s assessment, against an unknown DBT, is relevant to their own. This paper suggests that many aspects of a DBT will be very similar, for example it would be no great surprise if the author suggested that the UK’s DBT contained reference to vehicle and or person-borne explosive device(s), unmanned aerial systems, armed attackers, insider(s), indirect fire weapon systems, advanced cyber attack capabilities etc. A relatively straightforward assessment (especially compared to a zero base start point) targeted and focussed at particular perceived vulnerabilities, potential vital areas and considering high end threats described in its own DBT would enable an importing CA to confirm whether the assessment by the exporting CA is fit for purpose.

For the UK the safety-security interface is a mature consideration within the CA (it is the same CA for nuclear safety, security and safeguards). The UK IRRS mission in 2019 is a full scope mission and contains the safety-security interface module in full. Following an extensive self-assessment process (this aspect will be updated post the September 2019 mission) it is expected to recognise good practice in this area and importing CAs can derive benefit from the holistic nature of the
assessment undertaken by the UK ONR during GDA.

The overall aim is for the security community, which has for long been perceived as a blocker, to enable and support, but not promote (which is not the role of the CA), the peaceful use of nuclear power. Greater collaboration between CAs could enable the potential modularisation, rapidly deployable and scalable nature of the next generation of reactors to be realised.

State

United Kingdom

Gender

Male

**Primary author:** HASTED, Dan (UK Office for Nuclear Regulation)

**Presenter:** HASTED, Dan (UK Office for Nuclear Regulation)

**Track Classification:** PP: Nuclear security of new nuclear technologies (e.g., small modular reactors)
National Nuclear Security Regulation: Overview of Nuclear Cyber Security Requirements for NPPs

Abstract
We are living in a digital and information-driven age and need to store information related to virtually every aspect of our lives, nuclear information included. For computer system to be reliable and secure in nuclear facilities, unauthorized event changes must be prevented (which means maintaining confidentiality), field device inputs and outputs must remain immutable throughout their usable lifetime (which means maintaining integrity), and all component parts should remain in an operable state (which means maintaining availability). The dynamic and complex nature of cyber threats has made it a serious challenge to secure computer systems in nuclear facilities. A number of varied cyber security services, policies, mechanisms, strategies and regulatory frameworks have been adopted, including: confidentiality, integrity, availability, non-repudiation, encryption, defence-in-depth (DID), design basis threat (DBT), IAEA technical guidance documents such as: GS-R-1, GS-R-2, NSS13, NSS17, NST036, NST045, and NST047, IEEE standard 7-4.3.2-2010, NIST SP 800-53, NIST SP 800-82, NEI 04-04, NEI 08-09 and country-specific requirements such as: 10 CFR 73.54, RG 5.71 (U.S.NRC), KINS/RG-N08.22 (South Korea). However, threats remain persistent. This paper is aimed at providing an overview of regulatory standards and frameworks governing cyber security in nuclear power plants (NPPs) around the world, regulatory requirements and global best practice recommendations for nuclear cyber security, and strategies to prevent and counteract threats. This study is imperative as Nigeria prepares to join the league of countries with operational nuclear power plants and research reactors following approval and adoption of the nuclear power programme roadmap in 2007 and contract signing with Rosatom of Russia for NPP and research reactor construction.

Keywords: Cyber security, nuclear security, nuclear power plants, critical digital assets

State
Nigeria

Gender
Male

Primary author: Mr ARINZE, Uchechukwu (Information and Communication Technology (ICT) Unit, Department of Radiological Safety, Nigerian Nuclear Regulatory Authority (NNRA), South East Zonal Office, Enugu, Enugu State.)

Co-authors: Dr ENEH, Agozie (Computer Science Department, Faculty of Physical Sciences, University of Nigeria, Nsukka (UNN), Enugu,); Prof. LONGE, Babatunde Olumide (Department of Information Systems, School of Information Technology & Computing, American University of Nigeria (AUN), Yola, Adamawa State.)

Presenter: Mr ARINZE, Uchechukwu (Information and Communication Technology (ICT) Unit, Department of Radiological Safety, Nigerian Nuclear Regulatory Authority (NNRA), South East Zonal Office, Enugu, Enugu State.)
Models for Impact: Civil Society Engagement in Support of Nuclear Security

Nuclear security impacts everyone. Just as a nuclear accident anywhere is an accident everywhere, so too would a nuclear security incident anywhere be an incident everywhere. Though governments maintain that nuclear security is the responsibility of the state, the reality is that multiple stakeholders hold responsibility for nuclear security, from the legislators establishing laws that support nuclear security, to the regulators developing and implementing regulations, to the industrial, commercial and medical operators of nuclear technology. In that context, civil society can play an important role in supporting governments to strengthen nuclear security around the world. Civil society can provide valuable links between government and industry, raise awareness of the importance of nuclear security amongst different levels of stakeholders, and keep governments accountable to their commitments and for their actions.

The Nuclear Threat Initiative (NTI) has developed an impact model that enables it to work with governments around the world to reduce global threats, including nuclear security. This model involves four approaches, which can be conducted in different orders or simultaneously. The first is developing open source expert analysis about key nuclear security issues. This analysis can help identify good practices, gaps in activities, and potential methods to address those gaps. It also provides unclassified information that can be used to fuel discussions around the world. The second approach is to engage global stakeholders through meetings, workshops and seminars. These seek to stimulate collective self-interest and align essential forces worldwide to accomplish key goals and objectives. The third approach is to use direct action in specific circumstances that demonstrate innovative solutions to persistent problems. One example of the kind of direct action NTI has taken in the past includes providing the seed money to what became the Nuclear Security Fund, as well as initiating a project to assure supply of low enriched uranium (LEU), which is now the LEU Fuel Bank in Kazakhstan. Both of these projects started as a small input from civil society that then had large impacts and function self-sufficiently. Finally, the aim of our activities are to drive systemic change through institutional adoption of proven programs and practices.

Civil society activities using the approaches outlined above is an important contribution to international nuclear security. Civil society can bring creativity, innovation and flexibility to challenging problems, and provide opportunities for action that may not be available to governments. Additionally, civil society is an important link between governments, industry, and the general public, and help build strong support for nuclear security across sectors.

State
Other

Gender
Female

Primary authors: Ms HOLGATE, Laura (Nuclear Threat Initiative); BUFFORD, Jessica (Nuclear Threat Initiative)

Presenter: Ms HOLGATE, Laura (Nuclear Threat Initiative)
Track Classification: CC: Contribution of industry to nuclear security
DOES TIME MATTER FOR FRONT LINE OFFICER (FLO) IN CARGO ASSESSMENT TO DETERMINE THE PRESENCE OF NUCLEAR AND OTHER RADIOACTIVE MATERIAL OUT OF REGULATORY CONTROL? TRADE FACILITATION VS NUCLEAR SECURITY

Rusli, I.
Royal Malaysian Customs Department, Malaysia
Email: irfan.rusli@customs.gov.my

Abstract: Bureaucratic delays, excessive border procedure and inspection pose a burden for moving goods across borders for traders. Trade facilitation, which requires simplification, modernization and harmonization of export and import processes, has therefore emerged as an important issue for the world trading system. Trade facilitation plays an important role in promoting import, export, foreign direct investment and e-commerce, to ensure the economic growth of a country. Front line officer (FLO) such as Customs plays an important role in facilitating cross-border trade, whilst maintaining appropriate level of control and security. Various international legal instruments provide the framework on trade facilitation and security, such as The World Trade Organization (WTO) Trade Facilitation Agreement. Other inter-governmental organization such as The World Customs Organization (WCO) provide framework of standards such as the SAFE Framework of Standard in combating illicit trafficking including of nuclear or radioactive materials. To detect cargo that may or may not related to nuclear and other radioactive material out of regulatory control (MORC) is becoming challenging due to complexity of trade, and the assessment of commodity related to these materials. The detection system and measures is essential in filtering and detecting high-risk goods such as illicit trafficking of nuclear and radioactive material at the international borders. However, dedicated resources specifically deployed in monitoring the centralised alarm system (CAS) may no longer be feasible in this context of trade facilitation. Furthermore, the assessment of alarms, secondary inspections and response from technical experts added to the pressure for timely border clearance. This paper highlights the Time Release Study (TRS) conducted by the Royal Malaysian Customs Department at Port of Klang, 12th busiest port in the world which handles more than 11million containers (TEUs) per year. This study measure the time of cargo release at the border, which include the element of assessment and physical inspection of cargo related to nuclear and other radioactive materials. The results show that assessment and secondary inspections added to the time for border clearance. This paper calls for reform for nuclear security detection operation at border, to emphasise on the element of clearance time by focusing on high-risk cargo by using risk management approach as recommended by the WTO and WCO. Policy maker and international partners that support the implementation of nuclear security such as US-NSDD, European Commission, IAEA and other relevant international partners also need to consider the approach by the deployment of combination of Radiation Portal Monitor (RPM) and X-Ray instrument to optimise the FLO resources not only for nuclear security detection, but also for contraband commodities. Concept of centralise and dedicated CAS need to be reconsidered by merging the system and measure with existing Non-Intrusive Inspection (NII) control centre to optimise the decision making to expedite and facilitate legitimate good for border clearance. Finally, this study also demonstrates that TRS is a useful performance tool to measure time between the interface from detection, assessment and response from relevant authorities for the improvement of process flow and standard operating procedure (SOP).

Key Words: trade facilitation, nuclear security, assessment of alarms, time-release study, risk management.
State
Malaysia

Gender
Male

Primary author: Mr RUSLI, Amirul Irfan
Presenter: Mr RUSLI, Amirul Irfan

Track Classification: MORC: Preventing illicit trafficking of nuclear and radioactive material
Digital Hazards Identification: A New Approach to Cyber Security for Nuclear Facilities

The increasing use of digital instrumentation and control (DI&C) systems in nuclear power plants (NPP) presents new challenges to traditional security and protection measures. The current focus of cyber security-related research on protecting sensitive information or privileged networks from state-of-the-art “hacker” attacks struggles to adequately address protection needs for digital controls over physical processes. Thus, there is a need for cyber security research to move beyond an “anti-hacker” approach and more systematically identify and describe potential hazards that can be experienced in physical space but initiated (or implemented) in digital space. As is a common struggle across all cyber security efforts, the large number of potential failure modes from DI&C systems challenge the efficacy of deterministic approaches to identify critical digital assets or probabilistic risk assessments (PRA)-based analysis. This suggests that a risk-informed approach is necessary to properly assess the importance of DI&C systems to the criteria outlined in international cyber security best practices and better protect nuclear fuel cycles facilities (and activities) as pieces of critical global infrastructure.

Research funded by the Electric Power Research Institute (EPRI) in the U.S.—in collaboration with the Complex Hazards Analysis for Risk Management (CHARM) Team at Sandia National Laboratories—developed a response founded on key systems engineering concepts as “holistic” system characterization, describing new interactions enabled by DI&C, and illustrating interdependencies between DI&C and non-DI&C elements. Using these concepts, the CHARM team evaluated the appropriateness and adequacy of both traditional (e.g., Fault Tree Analysis, FTA) and novel (e.g., Systems-Theoretic Process Analysis, STPA) hazards analysis techniques for addressing these cyber security challenges. The CHARM team concluded that combining STPA and FTA leverages the benefits and overcomes the shortcomings of the individual methodologies to meet the criteria for risk-informed cyber security methodology—resulting in the Hazards and Consequence Analysis of Digital Systems (HAZCADS) technique. HAZCADS merges the system-theoretic principles of STPA with the probabilistic elements of FTA to efficiently and methodically identify, categorize, and assess hazards that can emerge from digital systems in NFC activities.

HAZCADS better incorporates both the direct and indirect roles of digital components in potential failure pathways and expand upon traditional cyber security approaches by incorporating: (1) the uniqueness and complexity of DI&C components; and (2) newly identified digital failure modes, including those from component interactions that still result with no component failure occurring. This paper will briefly summarize the core tenets of both FTA and STPA, provide a detailed description of how to develop SIFTs, and introduce the overall HAZCADS methodology. Next, a review of several examples of applying HAZCADS will be provided, including a comparison of lessons learned. Finally, this paper discuss several key implications for this new cyber security approach, including more effective application of limited cyber security resources on more vulnerable areas and higher fidelity (and flexible) digital hazard identification approach for NFC activities consistent with international best practices.


SAND
Gender

**Primary authors:** Mr CLARK, Andrew (Sandia National Laboratories); WILLIAMS, Adam (Sandia National Laboratories)

**Presenter:** Mr CLARK, Andrew (Sandia National Laboratories)

**Session Classification:** Identification, Classification, and Protection of Digital Assets in a Nuclear Security Regime

**Track Classification:** CC: Information and computer security considerations for nuclear security
Coordinated Research Project (CRP) for Improved Assessment of Initial Alarms from Radiation Detection Instruments

Sustaining and Strengthening Efforts – Improved Assessment of Radiation Portal Monitor Alarms at Laem Chabang Seaport
Aukrit Wongpanich, Natthawit Phiongam, Yanapan Hao
Thai Customs
Email: wongpanich1234@gmail.com
ABSTRACT
Thai Customs has several missions, including obligations to facilitate trades, collect tax, and protect the society. To ensure nuclear safety and security by detecting and deterring presence of illicit trafficking of nuclear and other radioactive materials, Thai Government participated in the Megaports Initiative Project with the United States Department of Energy to established an extensive network of radiation portal monitors (RPMs) at the Port of Laem Chabang, which is the largest seaport in Thailand.

The sensitivity of the RPMs is such that containerized cargo containing radionuclides of natural origin only occasionally cause alarms. In order to increase effectiveness of the current operation of the radiation detection system, Thai Customs, together with its co-authors, collaborated to acquire and utilize expertise and information that are not readily available, there is a need for better tools to help with this process.

In order to increase effectiveness of the current operation of the radiation detection system, Thai Customs, together with its co-authors, collaborated to acquire and utilize expertise and information that are not readily available, there is a need for better tools to help with this process. This paper will present results from the data collected from June 2018 to May 2019. The results significantly contributed to the current radiation alarm assessment.

State
Thailand

Gender
Male

Primary author: OFFICE OF ATOMS FOR PEACE, THAILAND
Co-author: LAEM CHABANG PORT CUSTOMS BUREAU, THAILAND
Presenter: LAEM CHABANG PORT CUSTOMS BUREAU, THAILAND

Track Classification: CC: Advances in nuclear security research and development; international cooperation on nuclear security research
Preliminary Results related to Human Factors Engineering Specifications for Advancing Radiation Detection Equipment’s

The current state of portable and handheld radiation detection instruments and systems used to detect a criminal or an unauthorized act with nuclear security implications involving nuclear or other radioactive material that is out of regulatory control is often inadequate to meet the nuclear security needs of the users within States. This paper focuses on one important, and often overlooked, aspect of the specifications for radiation detection equipment that leads to a mismatch in the operational needs for nuclear security operations and the equipment used.

Oftentimes, specifications for detection equipment are more focused on performance issues such as the library of isotopes, the dose rate measurement ability, etc. However, just as important to the user of the equipment is the ability to “hold” the handheld equipment in the position needed to take the required measurement. In the field, measurements are frequently taken that require physically unsupported arm positions and holding the equipment at odd angles for 2 to 5 minutes. Additionally, the outside conditions may be very hot, very cold, raining – each with their own clothing or other constraints that affect equipment holding times, and as a direct result the ability of the detection system to yield results. To address the gap between operational/human needs and the performance capabilities of the equipment, common system engineering principles can be applied. The interdisciplinary approach of systems engineering can enable the realization of successful systems. In this specific case, human factors must be considered as an important component to focus attention on the human element of the system and identify human performance requirements. A rigorous systematic approach should be used to identify critical interactions between people and equipment and thus mitigate negative impacts of the equipment itself on human performance.

Incorporating human factors early in design is also a cost-effective approach to maximizing the likelihood that a deployed instrument can provide a measurement under actual field and operational conditions, and by extension enhancing the sustainability of effective nuclear security detection activities. Mitigating human interface issues for an established system is more difficult than factoring in human capabilities and limitations in initial design. In some cases, performance (detection sensitivity, battery life, etc.) of the instrument has been sacrificed to reduce weight. In other cases, weight is not properly distributed for one-handed use or for long durations of carrying or holding in the expected use conditions. The use of equipment under field conditions should match the physical capabilities of the expected population of users (not just militarily fit 21 year old, 175 cm tall males in summer uniform) and support the measurement times and conditions under which performance will be effective. Equipment design should be assessed from a human interface perspective to help design engineers to create a better product. If the human interface is considered, the implementation of a State’s detection strategy will improve with more effective use of equipment and increase the probability of detection of radioactive materials out of regulatory control.

This paper provides some of the preliminary results of the research experiments studying the form and weight factors of different types of radiation detection equipment. More than 1000 experimental measurements have been taken using a diverse body of users and also simulation of various weather and clothing conditions. These measurements are providing important information about realistic times that users can hold up instruments given various weights and form factors (affecting the distribution of the weight around the hand). The results can support development of optimal equipment specifications using established systems engineering principles. Systems engineering is an interdisciplinary approach to enable the realization of successful systems. Human factors is an important component to focuses on the human element of the system, identifies human performance requirements for a successful system, identifies critical interactions between people and
equipment, Mitigates negative impacts of the environment on human performance.

All of the above described research activities have been done under the Coordinated Research Project (CRP) J02012 “Advancing Radiation Detection Equipment for Detecting Nuclear and Other Radioactive Material out of Regulatory Control” organized and supported by International Atomic Energy Agency (IAEA), Division of Nuclear Security, Department of Nuclear Safety and Security. Albania joined this CRP in 2017 and since then the Institute of Applied Nuclear Physics has been collecting data from a large number of research experiments examining different form factors and weights of radiation detection equipment under various use conditions.

**State**
Albania

**Gender**
Male

**Primary author:** Dr TUSHE, Kozeta (Institute of Applied Nuclear Physics)

**Co-authors:** Dr MASSEY, Charles (International Atomic Energy Agency); Dr PRIFTI, Dritan (Institute of Applied Nuclear Physics); Prof. BYLYKU, Elida (Institute of Applied Nuclear Physics); Dr DACI, Brunilda (Institute of Applied Nuclear Physics)

**Presenters:** Dr TUSHE, Kozeta (Institute of Applied Nuclear Physics); Dr MASSEY, Charles (International Atomic Energy Agency); Dr PRIFTI, Dritan (Institute of Applied Nuclear Physics)

**Track Classification:** MORC: Detection technology development and performance testing
BR2 LEU Conversion with High Density Silicide Fuel

As the Belgian Nuclear Science Center, SCK-CEN has been maintaining and operating the BR2 research reactor since 1962. The BR2 is one of the world’s most powerful and versatile research reactors with very high neutron dose rates and extensive experimental positions available for use. The three main utilizations of BR2 are: nuclear fuels and material research, the commercial production of radioisotopes, and the commercial production of doped silicon for high-grade semiconductors. The BR2 is essential for the European Union, and the world, for the security of critical medical isotopes, such as molybdenum-99. Since the BR2 operates with high enriched uranium (HEU), the Belgian government has voluntarily been supporting the minimization of HEU by developing a technically and economically feasible low enriched uranium (LEU) fuel for conversion of the BR2.

The United States has been pursuing the reduction or elimination of HEU around the world as a national program since 1978. Some of the early U.S. led efforts resulted in the licensing and LEU conversion of many research reactors on a new fuel type they developed: 4.8 g/cc loaded silicide (U3Si2) fuel. Over the past 15 years, SCK-CEN has been actively leading European efforts to convert high performance (high power and/or high neutron flux) research reactors to convert from HEU to LEU. These international efforts have been made in close coordination and cooperation with the U.S. Department of Energy efforts for LEU conversion and other key European partners. For some years, BR2 has been pursuing a LEU conversion path with a U-7Mo alloy fuel. However, recently it has become apparent that there is still significantly more to understand about the fuel performance behavior and the back-end solutions of the U-7Mo fuel before LEU conversion to this fuel type can be realized without significant risks. Recent BR2 LEU conversion focus has now shifted to a high density silicide fuel to build upon the extensive fuel performance history of the 4.8 g/cc silicide fuel and capitalize on the existing manufacturing and back-end solutions.

A BR2 LEU conversion project with high density silicide fuel at 5.3 g/cc loading was initiated and is well underway at SCK-CEN to pursue a more streamlined path to LEU conversion with significantly reduced risks than with U-7Mo fuel. The detailed plan has been established, internal approval and funding has been secured, and external contracts have been signed and are currently being executed. The BR2 LEU design is now complete and includes the 5.3 g/cc silicide fuel loading, the addition of a gadolinium burnable absorber, an increased fuel meat and fuel plate thickness, and a slightly modified fuel assembly to allow for the thicker fuel plates. Some changes have been incorporated into the HEU fuel assembly design now, to reduce risks and ensure a smooth transition and from HEU to LEU. The Gd burnable absorber and the physical assembly changes have now been implemented in irradiated HEU fuel assemblies with positive results. Additionally, work for the LEU fuel development of the 5.3 g/cc LEU silicide fuel is underway and the initial fuel plate irradiation is expected to be completed in mid-2020. Upon successful results of the 5.3 g/cc fuel plate irradiation, LEU BR2 fuel assemblies will be fabricated and the “Lead Test Assemblies” (LTAs) will be irradiated. These are necessary to complete the submission of the BR2 LEU conversion licensing package in 2025.

SCK-CEN is leading the way in the development and qualification of LEU high density silicide fuel. Other high performance research reactors such as the High Flux Isotope Reactor (HFIR) at Oak Ridge National Laboratory in the U.S. and the Réacteur nucléaire Haut Flux (RHF) at L’Institut Laue Langevin (ILL) are now investigating the possibility of a LEU conversion to high density silicide. As there are multiple parties interested from various countries, it is imperative that international cooperation and exchange continue for LEU conversion activities, such that a high density silicide fuel can be realized to ensure continued minimization of HEU throughout the world.

State
Belgium

Gender

Male

Primary author: Dr VAN DEN BERGHE, Sven (SCK•CEN Belgian Nuclear Research Centre)

Co-authors: Mr LANDERS, Chris (U.S. Department of Energy); WIGHT, Jared (SCK•CEN Belgian Nuclear Science Centre); Dr CHANDLER, David (Oak Ridge National Laboratory)

Presenter: Dr VAN DEN BERGHE, Sven (SCK•CEN Belgian Nuclear Research Centre)

Track Classification: PP: Minimization, on a voluntary basis, of high enriched uranium within civilian stocks and where technically and economically feasible
Assessing Progress on Nuclear Security Action Plans

Participants at the final Nuclear Security Summit in 2016 agreed on “action plans” for initiatives they would support by five international organizations and groups—the International Atomic Energy Agency (IAEA), the United Nations (UN), Interpol, the Global Partnership Against the Spread of Weapons and Materials of Destruction, and the Global Initiative to Combat Nuclear Terrorism (GICNT). The institutions were supposed to play key roles in bolstering ongoing nuclear security cooperation after the summit process ended. The action plans were modest documents, largely endorsing activities already underway, and there have been mixed results in implementing them.

For example:

• Some IAEA member states who were not invited to the summits have not wanted the IAEA’s nuclear security programs to be driven by decisions from a summit process they had no voice in. As a result, in pursuing its nuclear security work, the IAEA has generally—apart from publishing information circulars—not referred to the summits or the action plan. Most of the IAEA action plan simply committed participating states to “advocate” for the IAEA “continuing” to do things it was already doing, and those have continued. But it also called for enhancing “the importance of nuclear security” at the IAEA, for “reliable and sufficient resources” for the IAEA’s nuclear security work, and for participants to “periodically” host IAEA nuclear security reviews, and there has been only limited progress in these areas since the 2016 summit. The IAEA’s 2016 nuclear security conference made clear that the IAEA could serve as a crucial forum for discussions among experts, but was a challenging place for making political decisions about next steps. Countries made no new major new nuclear security commitments; the ministerial declaration was weaker than the statement from the 2013 ministerial; and very few countries made meaningful announcements about further progress.

• The Global Partnership’s action plan mentioned, among other initiatives, helping countries with nuclear security culture; reducing insider threats; strengthening transport security; strengthening computer security; and working with the nuclear security Centers of Excellence. Global Partnership participants have taken only very modest steps in these directions since the nuclear security summits. While the G7 and the Global Partnership it launched continue to discuss nuclear security, they have not attempted to take on any substantial part of the role the summits played in discussing and deciding on next steps in nuclear security.

• The GICNT action plan, like its IAEA and UN equivalents, largely endorsed activities already planned. Most of the work in the plan was focused on GICNT’s three working group areas, and not on physical protection or control and accounting for nuclear weapons, weapons-usable nuclear material, or high-consequence nuclear facilities—though the plan did suggest convening expert meetings to discuss possible activities “in other technical subjects or on cross-disciplinary issues” covered by the GICNT principles, and called for helping states build capacity “across the spectrum of nuclear security challenges.” There is little indication that the action plan has led to significant new activities in actually providing security for nuclear weapons, materials, or facilities.

• The Interpol action plan primarily endorsed activities already underway or planned. While the action plan did pledge that participants would contribute additional resources to Interpol’s nuclear and radiological efforts, there is little indication this has happened.

• The action plan for the United Nations largely reaffirmed the limited UN activities already taking place. Where the Action Plan mentioned specific new initiatives, the record on follow-through is mixed.

This paper will review the key nuclear security activities of these five international organizations and groups since the 2016 summit, and in what areas the action plans can be said to have led to action. It will then assess the barriers that exist to achieving the goals of the action plans in
these organizations. Finally, it will provide recommendations for how these five international institutions can make further progress in strengthening nuclear security around the world.

**State**

United States

**Gender**

Male

**Primary authors:** ROTH, Nickolas (Belfer Center, Harvard University); BUNN, Matthew (Harvard University)

**Presenter:** ROTH, Nickolas (Belfer Center, Harvard University)

**Track Classification:** CC: Use of IAEA and other international guidelines for building national nuclear security regimes
Toward a Game-Theoretic Metric for Nuclear Power Plant Security

Modern commercial nuclear power plants rely on the seamless integration of cyber components with underlying physical processes to achieve a profitable and safe operating environment. This integration of the cyber and physical worlds offers many improvements over traditional plant systems, such as advanced instrumentation and control techniques and improved system monitoring and diagnostics. While these technologies enable significant new capabilities, they can also introduce new vulnerabilities to plant systems.

Because the cyber and physical worlds are integrated, a successful cyber attack on a nuclear power plant could result in physical damage to the system, including severe consequences such as core damage. To protect a nuclear power plant, security engineers must determine which cyber and physical defenses are required, and the degree to which those defenses must be implemented. A method is desired to accomplish two objectives: (1) to quantify the security of nuclear power plants, and (2) to determine the defenses required to reasonably ensure the plant’s safe operation.

A game-theoretic approach is proposed to develop a security metric for nuclear power plants. Game theory is a mathematical technique used to analyze the interactions of multiple decision-makers, or players. Each player has a set of strategies from which to choose. The outcome of the game is dependent on the strategies selected by all the players. Each player receives a quantified utility that is dependent on the outcome of the game. At a Nash equilibrium of the game, all players have selected strategies such that their utilities have been maximized with respect to the other players’ strategies. Using game theory, we can determine which defense strategies to implement to optimize the outcome of the game.

This work applies game theory to quantify the security of nuclear power plants and prioritize security measures. The game will consider the interactions of an attacker who seeks to damage the system, and a defender who seeks to protect the system. The attacker incurs expenses to attack the system and receives a gain if the attack is successful. The defender incurs expenses to attack the system and incurs a loss if the attack is successful. Once the Nash equilibrium of the game has been determined, we can determine the probability of an undesirable outcome of the game. This probability can be compared to a desired security probability threshold to determine if the plant has been adequately protected.

It is assumed that the probability of a successful attack is dependent on the strategies selected by both players. This probability can be dependent on several factors such as the attacker’s knowledge of the system and the defender’s configuration of off-the-shelf components. By manipulating the factors that are within the defender’s control, the probability of an undesirable outcome can be reduced. The degree of implementation of a defense can be selected such that the probability of an undesirable outcome is less than the desired probability threshold.

The game-theoretic security technique is demonstrated on a simplified pressurizer system. Failure conditions are identified for the system using fault tree analysis. Economic parameters are assumed for the attacker and defender, and the Nash equilibrium is determined. The optimal defense strategy and degree of implementation are identified to achieve a required security probability requirement.

State

United States
Gender

Primary authors: LAMB, Christopher (Sandia National Laboratories); Mr MACCARONE, Lee (Sandia National Laboratories)

Presenters: LAMB, Christopher (Sandia National Laboratories); Mr MACCARONE, Lee (Sandia National Laboratories)

Track Classification: CC: Information and computer security considerations for nuclear security
Consolidation of nuclear security capacities in The republic of Moldova

Since the beginning of the implementation of IAEA INSSP, Moldova has achieved promising results in the context of strengthening security capabilities. Thus, the infrastructure for the detection of radioactive and nuclear materials at the border control points was strengthened, the system of physical protection of the nuclear and radiological facilities was strengthened. Also, the building of the national nuclear forensics capacity, the detection and the placement under control of orphan radioactive sources, the development of the regulatory framework in the field of nuclear security was developed and implemented. Now it is on working process the drafting of First respond system in case of nuclear or radiological events. A special compartment is also the securing actions of the radioactive sources from the eastern part of the Republic of Moldova (Transnistria).

State
Moldova

Gender
Male

Primary author:  Dr BALAN , Ionel (NARNRA)
Presenter:  Dr BALAN , Ionel (NARNRA)

Track Classification:  MORC: Building and maintaining nuclear security detection architecture
Protecting sensitive nuclear sites

In this communication, Electricité de France (EDF) and the Gendarmerie Nationale (French Military Forces) will provide an update of the organization we have in France since 10 years for the Physical Protection of EDF Nuclear Power Plants (NPP).

Protecting French NPP relies on sharing of responsibilities between the French State and Nuclear Plant Operator (NPO). The State defines the threats and the objectives in terms of protection, provides for intelligence gathering and intervention, as a supplement to the obligations incumbent on the NPO. The NPO has a requirement to deliver results based on a reference case of threats supplied by the state as well as with reference to regulatory requirements. The Design Basis Threat reference case is regularly updated by the French state and leads EDF to periodically review its security arrangements for nuclear facilities.

Today, EDF approach is based on the implementation of three keys concepts based in line with the IAEA Nuclear Security Series. In this communication we will present non sensitive’s progress achieved in these three keys concepts (technical, organizational and nuclear emergency response governance and crisis organization) during the last past years.

In France, to protect its 58 NPP, EDF has chosen a specific model, relying equipment for physical protection and human resources. It’s a Public-Private partnership defined in a specific convention agreement between EDF and the ministry of interior. In this particular case, the relevant state forces are financed by EDF.

First, it’s important to know that the organization rely on resources that are held by the private civil sector classified as EDF staff (site security personnel) and the public sector. In that particular case, dedicated response units, called ‘PSPG’ are missioned to respond to the highest levels of threat. As these are state forces, these response units also constitute the first-tier response coordinated by the French state. The Gendarmerie is also present as a territorial police force and provides the special forces from regional and national level. The advantage and the suitability of this model, which allows flexible coordination between the NPO’s resources and those of the state, was underlined by the members of the IPPAS mission that was held in France at the end of 2011.

In this communication:
- We will also focus on a few pragmatic examples such as the cooperation between EDF and French State, the design and management of access and, the computer security equipment room security upgrade.
- We will share a part of the return of experience in the security crisis management between EDF and the Gendarmerie.
- This conference will also focus on a few pragmatic examples about cooperation between EDF and the Gendarmerie to design protection measures for first-tier response and to design barrier protection such as fences and special doors.
- EDF human resource’s management process will also explain with EDF role in the French CoE.
- We will particularly present EDF major technical and organizational recent update for the minimization of the risk about insider threats.

State

France
Gender

**Primary authors:** TEXIER, L; DESCHAMPS, B.; DEROUET, VALERIE (EDF)

**Presenter:** TEXIER, L

**Track Classification:** CC: Establishing and formalizing nuclear security processes into integrated management systems
Role of the IAEA in Coordination of International Cooperation in the Area of Nuclear Security: Remarkable Collaborative Efforts and Programmes of the Agency and Russian Federation

This paper emphasizes capability of the IAEA to tackle a broad range of tasks in the area of peaceful use of atomic energy and its role in coordination of international cooperation and providing technical support to its Member States, upon their requests, in building their national nuclear security regimes. The paper notes importance and expresses support to this activity.

This paper recommends to take into account interests of Member States as fully as possible to guide international cooperation in area of Nuclear Security and to be flexible and open to dialogue for the common interest. This should provide for more effective and efficient utilizing human, financial and intellectual resources of Member States and the IAEA. It also notes necessity of compliance to such basic principles as exclusive responsibility of state for providing nuclear security on their territory; provision of assistance to the state at its request only; protection of sensitive information; preservation of recommendatory nature of documents on Nuclear Security.

Purpose of the paper is to enhance awareness of the IAEA Member States about available opportunities and programmes of the IAEA. For this purpose, it provides an overview of various mechanisms and projects that are implemented by the IAEA Secretariat with the Russian support and also gives some information about technical cooperation and assistance of Russia provided directly to the Member States in the area of Nuclear Security in compliance with all the IAEA recommendations and approaches. It gives examples of successful current cooperation and briefs on plans for further interactions. It describes principles and priorities that Russia consider while providing support to the IAEA Secretariat activities.

State

Russian Federation

Gender

Not Specified

Primary authors: KOZLOVA, Nadezhda (State Atomic Energy Corporation ROSATOM); Mr ULANOV, Dmitry (State Atomic Energy Corporation "Rosatom"); LEBEDEV, Gleb (State Atomic Energy Corporation "Rosatom", Russian Federation)

Presenter: KOZLOVA, Nadezhda (State Atomic Energy Corporation ROSATOM)

Track Classification: CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
Status of Security of Transport of Radioactive materials in Ghana

With the increase in the application of radiation sources in various fields such as medicine, agriculture, research, and especially in industry, the transport of radioactive material has increased over the years which involves the movement of radioactive material from the port of entry to the storage facility of clients, from storage to the place of use, from one place of use to another place of use including offshore for the oil and gas companies and from the place of use to the agency responsible for the safe disposal. In Ghana, Ten (10) private companies have been licensed to transport sources with varying activities. The Nuclear Regulatory Authority (NRA) is the national regulatory authority for enforcement of the regulations for safe handling of radiation sources and transport of radioactive materials. The transport of radioactive material in Ghana is governed by the draft regulations i.e. Safe transport regulations of radioactive materials and well logging regulations which is based on IAEA regulations for ‘Safe Transport of Radioactive Material’ SSR-6, 2012 Edition.

The NRA has also prepared a draft regulation titled ‘Security of Radioactive Material during Transport’. The draft regulations establishes security levels commensurate with the potential radiological consequences that could result from malicious use of radioactive material. The objective of this document is to regulate and provide guidance, to an authorized user of radioactive material, consignor, carrier and other concerned persons, in implementing, maintaining security in order to protect radioactive material while in transport against theft, sabotage or other malicious acts that could result in significant radiological consequences. These processes when duly implemented will complement the country to safely and securely continue to transport radioactive materials in the country.

State

Ghana

Gender

Male

Primary author:  OBENG, Michael Kojo Asabre (Nuclear Regulatory Authority, Ghana)

Presenter:  OBENG, Michael Kojo Asabre (Nuclear Regulatory Authority, Ghana)

Track Classification:  PP: Transport of nuclear and other radioactive material: practices, challenges and regulatory issues
Cyber Security of Structure, System and Components Important to Safety

Cyber-attacks on industrial installations including nuclear power plants (NPPs) are a significant issue. Digital control systems are now at the core of industrial installations, playing a critical role in safety in many sectors, including Structures, systems, and components (SSCs) important to safety in the nuclear sector. The function of SSCs important to safety is to bring into a safe state when a fault occurs in the nuclear installations. Moreover, in the event of SSCs important to safety failure, the SSCs important to safety is expected to force the state of nuclear installation into its fail-safe condition. The architecture of SSCs important to safety need to be selected properly to enable safety function as designed.

Along with the various gains in flexibility and efficiency of digital systems, this evolution comes with new risks of digital attacks, exploiting a growing connectivity and reflecting recent changes in the threat landscape. Intrusion by an external or internal malicious attacker could violate the confidentiality, integrity, or availability of data. Even if the computers were not connected to the internet or air-gapped from the internet, attackers can devise scheme to infiltrate companies to get inside the system. The SSCs important to safety of the nuclear installations are potentially vulnerable to cyber attacks. After the appearance of Stuxnet, the safety assurance against cyber-attacks has been a serious problem for nuclear installations. With this vulnerability, it is proposed that SSC security risk assessment. Safety analysis procedure usually doesn’t include cyber security aspects. Safety and security are highly related concepts. They share the same goal—protecting the SSCs important to safety from failing. Both deal with the protection of public and environment from radiological consequences, and both do this by avoiding, detecting, and responding to incidents that can cause such consequences.

Cybersecurity has become more critical these days and to address such concern, risk assessment for the security of the SSCs important to safety is proposed to be included in the design and evaluation, as part of the enhancement process. An important step to proactively include and align cybersecurity risk assessment against hacking, malware or any cyber threats in the design and evaluation of the SSCs important to safety is proposed. Hazards and threats that can cause or enable such incidents to occur are identified and the associated risks are analyzed in order to ensure that these risks are mitigated to acceptable levels. In this case hardware architecture of SSCs important to safety should fulfill new requirements.

State
Indonesia

Gender
Male

Primary author: Mr JUSUF, Farid Noor (BAPETEN)
Presenter: Mr JUSUF, Farid Noor (BAPETEN)
Track Classification: CC: Information and computer security considerations for nuclear security
International standards for the performance of radiation detection instruments used in the global nuclear security framework

The physical protection of nuclear material is fundamental to nuclear security. Interdicting the illegal movement and transfer of nuclear material is part of the nuclear material physical protection. The instruments for monitoring the illegal movement of nuclear and radioactive material need to have performance characteristics and reliability that will assure that they will do the task of preventing the illegal movement and contraband of nuclear material. The minimum performance requirements that each type of radiation detection instrument must meet are specified in a set of standards. The international standards for radiation detection instruments are developed by the International Electrotechnical Commission (IEC) Sub-Committee 45B "Radiation Protection Instrumentation". The IEC is the oldest standards organization with more than 200 Technical Committees and Sub-Committees and over 20000 experts from all over the world. The IEC standards specify the minimum performance requirements for such instruments.

The international standards for detecting and monitoring the illegal trafficking of nuclear and radioactive material cover the following types of instruments:
1. Hand-held and portable instruments
   - Hand-held radionuclide identification devices
   - Hand-held highly sensitive photon devices
   - Hand-held highly sensitive neutron devices
2. Instruments worn on the body
   - Alarming personal radiation devices (PRD);
   - Spectroscopy-based alarming personal radiation devices (SPRD);
   - Backpack based radiation detector (BRD)
3. Instruments on Portals
   - Portal Monitors (RPM);
   - Spectroscopy-Based Portal Monitors (SPRM)
4. Instrumentation mounted on vehicles and used for drive-by monitoring
   - Vehicle-mounted mobile systems

The international standards specify requirements for the design and the general and radiation characteristics, the test procedures that show compliance with the standard requirements, as well as the electromagnetic, mechanical, climatic and safety requirements.

The criteria and compliance test methods in these standards are the result of consensus among the participating experts from many countries. The international standards reflect the positions of the national regulatory agencies, scientific and technological progress of the industry, testing laboratories capabilities, end user needs, testing cost and the way the instruments are used in the field.

The IEC/SC 45B standards for evaluation of the illicit trafficking of radioactive material control instrumentation are used in many countries. They have been transposed by the CENELEC/TC 45B as European EN standards which allows to be referenced and used in different projects and conformity assessment programs as the ITRAP (Illicit Trafficking Radiation Assessment Program). The US ANSI (American National Standard Institute) standards of the N42 group "Homeland Security Instrumentation" and the IEC/SC 45B standards are constantly being harmonized with each other.

The presentation provides overview of the IEC international standards for radiation instrumentation used for detection of illicit trafficking of radioactive and nuclear material.
State

Other

Gender

Male

Primary authors:  VOYTCHEV, Miroslav (IRSN);  Dr RADEV, Radoslav (LLNL)

Presenter:  VOYTCHEV, Miroslav (IRSN)

Track Classification:  MORC: Preventing illicit trafficking of nuclear and radioactive material
Abstract: The stable operation of the ICS (ICS) directly affect the safety of nuclear power plants and cyber security has become an important factor affecting nuclear safety. With the continuous development of the digitalization and networking of modern industry, the cyber security of ICS in nuclear power plants is facing unprecedented challenges. Therefore, it is necessary to take cyber security into consideration from the construction stage in nuclear power plants. From the perspective of the business owner, we analyze the cyber security risks faced by ICS during the construction phase and propose the technical defense architecture for newly built and being built nuclear power plants respectively combining the related international standards and guidelines. Further, we propose to build ICS cyber security test platform to verify the feasibility of the defense architecture.

1. Introduction
It was considered in the past that the ICS of nuclear power plants was relatively safe because it was isolated with outsider world and used specialized hardware and software to run proprietary protocols. However, with the higher degree of industrial digitalization and networking, the Windows platform and industrial Ethernet based on IEEE802.3 have been widely used in ICS. The ICS become open and face unprecedented security threats. From the “Stuxnet” incident in Iran to the recent power blackout in Venezuela, the cyber security of ICS in power plants is facing more and more challenges. Cyber security has become an essential part of production safety and the key ICS of a nuclear power plant will directly cause reactor shutdown events, which will lead to nuclear safety issues. Therefore, it is necessary to take cybersecurity into consideration from the construction stage, analyze the cyber security risks during the construction phase, and build targeted technical protection solutions for under construction and new nuclear power plants.

2. Related standards
2.1 RG 5.71
2.2 IAEA NSS
2.3 IEC 62443
2.4 IEC 62645
2.5 IEC 63096

3. Cyber security risk analysis of ICS in the construction stage of nuclear power plant
3.1 requirements for cyber security in nuclear power project management
This chapter introduces the main works of construction stage in nuclear power plants and analyzes the cyber security requirements in “information and document management” which is one of the seven fields of nuclear power project management.

3.2 Critical Digital Assets Identification
According to the requirements of RG 5.71, this chapter addresses how to identify the critical digital assets of ICS in nuclear power plant.

3.3 external threats analysis of critical ICS
This chapter analyzes the external threats to the critical digital assets identified in 3.2(critical ICS,) in the construction phase of nuclear power plants.

3.4 vulnerability analysis of critical ICS
This chapter analyzes the possible vulnerability of critical digital assets identified in 3.2 during the nuclear power plant construction phase.

4. Technical defense architecture research

Because of the long construction cycle of nuclear power plant, it will take huge cost to change the defense architecture after it was confirmed in the design phase. Therefore, this chapter studies the cyber security defense architecture of ICS in newly built and being built nuclear power plants respectively.

4.1 Technical defense architecture for critical ICS in newly built nuclear power plants

In this chapter, we propose the technical defense architecture based on trusted computing for critical ICS in newly built plants. We analyze the difference between trusted computing and traditional defense method, and explore how to use trusted computing technology to construct a defense architecture with active immune function.

4.2 Technical defense architecture for critical ICS in nuclear power plants being built

Because of the insufficient design of cyber security, we must take the cost and schedule into consideration as for the defense architecture for plants being built. We propose a semi-active defense architecture based on network isolation, protocol analysis for ICS and intrusion detection technology, which can detect and block threats in time.

4.3 Cyber security test platform for ICS in nuclear power plants

ICS have high requirement for high availability and some ICS with real-time control function, such as the protection system, will directly cause reactor shutdown events. Therefore, the cyber security technical defense architecture of critical ICS must be fully tested and verified. In this chapter we introduce the digital twin technology, and discuss the feasibility and advantages of constructing the cyber security test platform for ICS based on digital twin technology.

5. Conclusion

6. References
A cyber-capability model for compromise of I&C system functions at nuclear facilities

IAEA Nuclear Security Series No. 33-T provides an ordered list of the four potential consequences of a compromise on I&C system function are arranged from worst to best case. These potential consequences are the basis on which to define the computer security requirements for the I&C system functions. IAEA NSS 20 details the need for risk informed approaches to take into account a current assessment of nuclear security threats (i.e. threat actors having intent, motivation, opportunity, and capability to attack a State’s nuclear security regime). This need requires understanding of the cyber-capabilities on which to perform a detailed analysis to determine the security requirements.

This analysis can be supported by modelling threat actor capabilities required to compromise I&C system function via cyber-attack. This paper will propose a three-level capability model for use in evaluation of potential consequences and their likelihood of occurrence.

In this model, the threat actor capabilities lead to a classification into one of three “hacker” groups. They are IT hackers, ICS hackers, and nuclear process hackers. IT hackers have knowledge and understanding on how to compromise information technology and could initiate or target cyber-attacks on I&C systems that are likely to be more disruptive (i.e. failure) than causing more severe consequences. This is due to the attribute that IT hackers are not aware of the specialized characteristics of industrial control systems.

On the next level representing increasing threat, ICS hackers have the same capability as IT Hackers (having acquired the general knowledge of information technology) but they also have acquired the specific knowledge of industrial control systems.

On the level representing the highest threat, nuclear process hackers have the same capabilities as ICS hackers, but also have gained the access and understanding of the detailed information about I&C systems at nuclear facilities that they have targeted.

In this model, the different types of attacks are associated with each of the different types of threat actors. Application of this model, reveals that consequences increase in severity as the threat actor behind the compromise progresses from lower threat level (i.e. IT hackers) to the highest threat level (i.e. Nuclear Process Hackers). The three-level model proposed in this paper could also be utilized in development of a more sophisticated model used to develop the cyber design basis threat (cyber-DBT) of nuclear facilities.

State

China

Gender

Primary authors: LI, Jianghai (Institute of Nuclear and New Energy Technology, Tsinghua University); ROWLAND, Michael (Practical Reason Incorporated); HEWES, Mitchell (IAEA)
Presenter: LI, Jianghai (Institute of Nuclear and New Energy Technology, Tsinghua University.)

Track Classification: CC: Information and computer security considerations for nuclear security
Effective Opportunities for Gender Equality, Career Advancement, and Knowledge Building: Serving as a Chief Scientific Investigator

Opportunities within technical fields may seem limited for women, particularly in specialized areas such as nuclear security. There may be real or perceived barriers to career advancement, specifically in opportunities for women to exercise project or team management leadership, build important networks, and expand and demonstrate technical skills. This paper will discuss serving as a Chief Scientific Investigator of a research project as a very real mechanism to effectively address gender equality issues and to build capacity within Member States.

The IAEA encourages and assists research on, development of, and practical use of atomic energy and its applications for peaceful purposes throughout the world. It brings together research institutions from Member States to collaborate on research projects of common interest through Coordinated Research Projects (CRPs). For each project, participating institutes designate one staff member as the Chief Scientific Investigator (CSI) to manage the research project. The IAEA acts as the sponsoring and coordinating body; and an IAEA technical staff member is assigned to lead each CRP as the project officer.

A wide range of CRP activities yield diverse outputs, which include:
- Establishment of networks and databases;
- Development of tools to improve Front Line Officer performance effectiveness; and
- Development of devices or tools for equipment diagnosis and testing.

Sri Lanka has participated in many IAEA CRPs and I serve as the CSI for the CRP on Improved Assessment of Initial Alarms from Radiation Detection Equipment. This experience has greatly enhanced my technical acumen, project management skills, and leadership abilities. I will share how I have been able to lead a team, develop a network, and build my confidence.

The CSI role has also given me the opportunity to assist other Member States in the development and implementation of radiation detection strategies. For example, I led an expert mission to Cambodia to collect data and lead the development of a site-specific tool to improve consistency, accuracy, and efficiency of alarm assessments using the Tool for Radiation Alarm and Commodity Evaluation (TRACE). I have also participated in IAEA technical meetings to further my understanding of testing processes for radiation detection equipment. As a CSI I have benefited from mentorship and technical collaboration with the IAEA Project Officer. As a result, I have further developed my career while increasing effectiveness and sustainability of nuclear security detection activities in Sri Lanka.

As a woman, scientist, and nuclear security professional, I encourage women interested in enhancing their own and their State’s capabilities to participate in a relevant Coordinated Research Project.

State

Sri Lanka

Gender

Female
Primary author: Ms RATHNAWEERA, Nirasha (Sri Lanka Atomic Energy Board)
Presenter: Ms RATHNAWEERA, Nirasha (Sri Lanka Atomic Energy Board)

Track Classification: CC: Capacity building (e.g. human resource development and sustainability, nuclear security education and job-specific performance training including for newcomer countries)
Enhancing Sustainable Nuclear Security Operations through Participation in the Coordinated Research Project on Improved Assessment of Initial Alarms

Nuclear security is the responsibility of a Member State. Meeting international obligations and effectively implementing national nuclear security strategies can be a challenging activity, often-times made complicated by the need to implement and sustain national detection strategies that use both instruments and information. This paper will focus on the challenges of nuclear security operation involving detection by instruments and demonstrate how participation in an IAEA Coordinated Research Project (CRP) has directly led to the advancement of operations and enhanced the sustainability of nuclear security detection operations in Sri Lanka.

Sri Lanka is an island country with its seaports serving as a vital national economic and security connector to the global community. Not only does the major port of Colombo serve as a gateway for commerce into and out of Sri Lanka, the seaport also serves as an important gateway for east-west transshipment of goods. The security of commerce through the seaport is globally important, and Sri Lanka is proud of its efforts to ensure the nuclear security of cargoes moving through the part to reduce the likelihood of illicit trafficking in nuclear and other radioactive materials, and also to ensure the safety of cargo moving through the port.

Sri Lanka has installed and operates a sophisticated system of radiation detectors at the seaport to monitor cargo – providing nuclear security detection capacity and safety to ensure that radioactively contaminated goods and/or radiological sources out of regulatory control are detected and safely removed from commerce. The Sri Lanka Atomic Energy Board (AEB) and Sri Lanka Customs are two of the agencies involved in the detection operations and were faced with numerous sustainability challenges ranging from equipment sustainability, training, expert knowledge of equipment, and nuclear security culture.

To address a number of these challenges, the AEB and Customs decided in 2015 to join the IAEA Coordinated Research Project on Improved Assessment of Initial Alarms from Radiation Detection Equipment. The participation in this CRP has yielded benefits far beyond the initial expectations. The improvement in alarm resolution processes through the use of a Tool for Radiation Alarm and Commodity Evaluation (TRACE) has resulted in more effective, efficient, and consistent alarm resolution and improved training.

The participation in the CRP has also enhanced collaboration and expert knowledge among the stakeholders of national nuclear security regime through:

- Sharing technical knowledge and onsite experience (FLO/ Experts),
- Training implementation,
- Development of methodologies, and
- Improvement of detection capabilities.

The feedback for questionnaires distributed among the FLO’s on the use of TRACE in their alarm assessment activities will be included in the paper.

Sustainability of nuclear security culture in Sri Lanka has been enhanced through:

- Improved utilization and understanding of detection instruments and how to repair, maintain, and calibrate the instruments for peak performance,
- Improved and focused training using need analysis and a systematic approach to training (SAT).
• Improved Standard Operation Procedures (SOPs) that take advantage of the TRACE tool and have ensured a consistent and reliable source of information,

• Development of new approaches to implementing effective nuclear security detection operations.

Another important, and often overlooked benefit of participation in IAEA CRPs, is the enhanced opportunities for international collaboration. The CRP has provided an excellent pathway for the following:

• Sharing knowledge, experience and best practices through:
  • Technical & Scientific Visits among other CRP members,
  • Technical workshops to share enhanced alarm and data analysis capabilities, and
  • Interactions with technical experts and equipment manufacturers.

• Joining professional and nuclear security networks (IAEA- FLO, IAEA-NSSC, World Custom)

In summary, the participation in the CRP on Improved Assessment of Initial Alarms has had great positive impact on the nuclear security capacity of Sri Lanka. The tangible benefits have been discussed and the enhanced knowledge and skills will help sustain an effective nuclear security detection. Sri Lanka expresses its gratitude to the IAEA for the support and opportunity to participate in the CRP program. Sri Lanka encourages other Member States to join CRPs and for the IAEA to continue this very successful program that addresses Member States needs through mutual participation and capacity building.

State
Sri Lanka

Gender
Female

Primary author:  Ms RATHNAWEERA, Patabedige Nirasha Gayani (Radiation Protection & Technical Services Division, Sri Lanka Atomic Energy Board)

Co-authors:  Mr MAHAKUMARA, Prasad Dhananjaya (Radiation Protection & Technical Services Division, Sri Lanka Atomic Energy Board); Mr LIYANAGE, Indunil (Sri Lanka Customs); RANASINGHE, Nirodha (Radiation Protection & Technical Services Division, Sri Lanka Atomic Energy Board); IAMSUMANG, Chonlagarn (IAEA); Mr MASSEY, Charles (IAEA)

Presenter:  Ms RATHNAWEERA, Patabedige Nirasha Gayani (Radiation Protection & Technical Services Division, Sri Lanka Atomic Energy Board)

Track Classification:  MORC: Preventing illicit trafficking of nuclear and radioactive material
Effective Fuzz Testing for Programmable Logic Controllers Vulnerability Research to Ensure Nuclear Safety

Critical infrastructure, such as nuclear power plants, widely uses various Operational Technology (OT) solutions, such as Industrial Control Systems (ICS). OT networks used to be logically and physically isolated from other business functions, but nowadays it is not always true. Along with the digitalization of such systems, they got interconnected and internetworked. Thus new cybersecurity threats were introduced.

In the case of critical infrastructure, even the smallest disruption can cause undesirable, hazardous outcome. An action, as simple as changing a value of a single variable (e.g. temperature sensors readings) can result in serious damage to the pump control or whole cooling system. The key components of such OT networks are programmable logic controllers (PLCs), which process information about the physical process in order to manipulate it. PLCs are an inseparable part of 80% of ICS designs, thus their robustness has a direct, incontestable impact on the safety of the whole control systems. Some of the publicly reported incidents involving PLCs are: Stuxnet worm attack on Iranian nuclear facilities (2010) that reprogrammed PLCs to operate incorrectly resulting in failure of many centrifuges and an incident in Browns Ferry nuclear plant in Alabama, where a faulty PLC overloaded the network with excessive traffic. Therefore PLCs have been chosen as an object for our studies.

One of the methods commonly used in the security industry to look for vulnerabilities is fuzz testing. It is considered to be one of the most popular vulnerability discovery techniques. It owes its popularity to relatively high accuracy, good scalability as well as easiness of implementation of the method. The fuzzing technique is based on creating a purposely malformed input, delivering it to the target software and checking for failures. It can be applied to communication protocol testing at various stack levels. The rationale behind using this method is the belief that it offers unmatched ability to quickly test a wide range of cases.

There is a need to refine fuzz testing methodology for the purpose of security testing of PLCs used in nuclear industry. Therefore this paper aims to answer the following research question: To what extend fuzz testing can be used to find zero-day vulnerabilities in programmable logic controllers commonly used in nuclear industry?

In order to answer the posed research question, specialized laboratory, consisting of several PLCs and a fuzzing tool, was created. Additionally, an existing fuzzing methodologies were reviewed and improved for the purpose of PLC testing. Especially, taking into regards its limitations in terms of data access. Using the built testbed and methodologies, two different models of Siemens PLC were examined regarding robustness of different network protocols implementations. During conducted research several vulnerabilities were found, including a zero day vulnerability in Siemens S7-1500 PLC.

This paper presents requirements for fuzzing laboratory, fuzzing methodology focused on PLCs, and analysis of the found vulnerabilities. This research has been carried out in Nuclear Centre for Nuclear Research (Poland) as a part of IAEA Coordinated Research Project (CRP) J02008 in incident response in nuclear facilities.
Gender

**Primary authors:** SUCHORAB, Jakub (National Centre for Nuclear Research); Ms WALKIEWICZ, Joanna (National Centre for Nuclear Research); Ms STASZKIEWICZ, Kinga (National Centre for Nuclear Research); Mr DUDEK, Marcin (National Centre for Nuclear Research)

**Co-author:** Dr GAJEWSKI, Jacek (National Centre for Nuclear Research)

**Presenters:** SUCHORAB, Jakub (National Centre for Nuclear Research); Ms STASZKIEWICZ, Kinga (National Centre for Nuclear Research)

**Track Classification:** CC: Information and computer security considerations for nuclear security
Production of three uranium ore concentrate certified reference materials

Synopsis of the technical paper to be presented at the:

International Atomic Energy Agency International Conference on Nuclear Security: Sustaining and Strengthening Efforts
IAEA Headquarters, Vienna, Austria
10-14 February 2020

Prepared by:
K. Nadeau
Inorganic Chemical Metrology
NRC Metrology Research Center
National Research Council Canada
Ottawa, Ontario, Canada

Z. Mester
Inorganic Chemical Metrology
NRC Metrology Research Center
National Research Council Canada
Ottawa, Ontario, Canada

A. El-Jaby
Directorate of Security and Safeguards
Canadian Nuclear Safety Commission
Ottawa, Ontario, Canada

Synopsis

As part of the Government of Canada’s broader efforts to enhance and expand its nuclear material provenance assessment capabilities, the Inorganic Chemical Metrology (ICM) team of the National Research Council Canada (NRC) was tasked with producing uranium ore concentrate (UOC) certified reference materials (CRM) to support advanced measurement and characterization activities of front-end nuclear fuel cycle materials. Three candidate UOC materials, each with a unique chemical composition profile and ranging in uranium content from 0.80 g/g to 0.85 g/g. Being an industrial material, these UOCs had to be crushed, sieved, dried, homogenized and individually bottled. A representative number of bottles from each CRM have been selected during the bottling process and have been used for the certification campaign. Measurements for the analytes of interest include a) uranium content; b) isotope ratios of U, Sr, Pb, and Nd; c) S, C, H, N, O, and C content; d) isotope deltas of H, C, N, O, and S; e) trace element impurities; f) accelerator mass-spectrometry measurements of 236U, 231Pa, 230Th, and 226Ra, leading to the reported values for 236U/238U and estimates of 231Pa/238U, 230Th/238U, and 226Ra/238U; g) measurements of anions, including chloride, fluoride, nitrate, phosphate, and sulfate; and h) physical characteristics such as particle size, shape, density, colour, and Raman signature. This paper will summarize the analytical procedures that led to the certification of the three UOC materials produced by NRC.

State

Canada
Gender
Male

Primary authors: Mr NADEAU, Kenny (NRC Metrology Research Center National Research Council Canada); Mr MESTER, Zoltan (NRC Metrology Research Center National Research Council Canada); Mr EL-JABY, Ali (Directorate of Security and Safeguards Canadian Nuclear Safety Commission)

Presenter: Mr NADEAU, Kenny (NRC Metrology Research Center National Research Council Canada)

Track Classification: MORC: Nuclear forensics
Development, Implementation, and Sustainability of a National Nuclear Forensics Library Capability to Address Nuclear and other Radioactive Material out of Regulatory Control

Summary
The extended abstract provides a historical context and overview of a National Nuclear Forensics Library, henceforth 'Library', summarizes outcomes of the technical session on Libraries from the 2019 IAEA Technical Meeting on Nuclear Forensics: Beyond the Science, and offers an outlook of Library development, implementation, and sustainability over the next ten years.

Description
In support of an investigation of nuclear or other radioactive material found out of regulatory control (MORC), nuclear forensics provides technical information useful for identifying MORC and determining its provenance in the context of international legal instruments and national laws related to nuclear security. A Library is one mechanism for evaluating data from a nuclear forensic examination to determine if MORC is consistent with materials used, produced, or stored within the borders of the State in which it was recovered. This is critical information for investigators, both for identifying and addressing potential nuclear security issues within a State’s borders, or, if it appears MORC originated from another country, provides a mechanism for queries and dialog with other possible source countries.

The creation of Libraries has been supported by the IAEA, Nuclear Forensics International Technical Working Group (ITWG), the Global Initiative to Combat Nuclear Terrorism (GICNT), and the Nuclear Security Summits, but development internationally has been slow, due to the complexity of the task to develop, maintain, and sustain a Library in a national context.

While the impetus for the development and use of a Library in support of nuclear forensics examinations have been a consistent theme at the policy making level, mechanisms for Library implementation and use for the identification of MORC is something richly debated. The IAEA publication, Development of a National Nuclear Forensics Library: A National System for the Identification for Nuclear or Other Radioactive Material out of Regulatory Control, provides policy makers, competent authorities, law enforcement officials, and technical personnel with information about the role and benefit of establishing and using a Library as part of a nuclear security investigation and imparts context for the use of a Library to identify the origin and history of MORC. More specifically, it provides information helpful to understand where to find and how to organize the technical expertise and data resources needed to successfully implement a Library, and mechanisms for how to seek the international cooperation or assistance sometimes necessary to identify MORC.

While guidance is available from the IAEA, Member States highlighted, as part of the 2019 IAEA Technical Meeting on Nuclear Forensics: Beyond the Science, that Libraries, although driven by the same goal, are not implemented in the same fashion globally, and Member States are choosing unique approaches to developing, maintaining, and sustaining a Library. Presentations given at the 2019 Technical Meeting highlighted that there is no 'one-size fits all' methodology for Library development, but all participating parties supported the basic concepts that a country should be able to use nuclear forensic examination data to identify materials from their holdings, and be prepared to engage international partners if necessary to support a nuclear security investigation involving MORC.

Looking forward over the next ten years, more states are expected to develop a Library as part
of their domestic nuclear security program. The diversity in how states organize or access the data and subject matter expertise necessary to assess provenance will continue to grow as the Library concept continues to gain broader acceptance as a critical capability for supporting MORC investigations. This diversity is a recognition that no single prescriptive approach to implementing a Library and method for requesting assistance from international partners is appropriate, and each state must decide how to ensure they have a robust mechanism for determining if MORC is consistent with domestic holdings.

State
United States

Gender
Male

Primary author:  LAMONT, Stephen (United States Department of Energy)
Co-authors:  DAVYDOV, Jerry (International Atomic Energy Agency (IAEA)); CURRY, Michael (U.S. Department of State)
Presenter:  LAMONT, Stephen (United States Department of Energy)

Track Classification:  MORC: Nuclear forensics
Legal considerations for the application of nuclear forensics in the context of nuclear security

Nuclear forensics is a multidisciplinary field where science meets law. While the conduct of a nuclear forensic analysis requires advanced scientific capabilities, the ultimate purpose of the forensic investigation is to deliver reliable and relevant evidence for a number of purposes, including in legal proceedings. Nuclear forensic capabilities are not established in a legal vacuum: their application in legal proceedings finds its foundation in national legal frameworks that criminalize unauthorized acts related to nuclear and other radioactive material. In addition, nuclear forensics support the implementation of measures required by the international legal framework related to nuclear security.

International legal instruments for nuclear security, such as for example the International Convention for the Physical Protection of Nuclear Material (CPPNM) or the International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT), create a number of obligations relevant for the application of nuclear forensics. In particular, they create obligations that require States to:

- create offences in relation to specified intentional actions involving the misuse of nuclear and other radioactive material
- prosecute said offences
- implement mechanisms for cooperation as well as for requesting, receiving and providing assistance with the investigation of nuclear security events

Furthermore, numerous legal considerations have to be taken into account in connection with a nuclear forensic investigation. They amount, on the one hand, to provisions related to admissibility of evidence (1) and, on the other hand, to provisions related to the regulatory framework for the safe and secure handling of analysed material (2):

1. Procedures and methods are established for the admissibility of traditional forensic examinations in a courtroom; similar legal requirements apply to nuclear forensic examinations. The management of a nuclear forensic investigation must answer to rigorous requirements of prosecution. It is subject to the same rules as traditional forensic evidence but raises a number of additional challenges due to the inherent nature of the material. Rules of collection and handling of evidence, chain of custody, confidentiality, the preservation of evidence and documentation and the means of reporting findings should all have a sound basis within the legal system of each individual country which possesses and uses nuclear forensics capabilities.

2. The national legal and regulatory framework should support and empower competent authorities with a role in nuclear forensics so as to ensure that their roles and responsibilities for nuclear forensics in relation to nuclear security events are clearly defined. It should also contain adequate provisions for implementing nuclear forensic capabilities (national response plan, etc.), as well as for the safe and secure storage of evidence and transport. These are often provisions to be found in nuclear legislation, but their applicability to nuclear forensics should be ensured and adapted when necessary.

The paper will focus on legal considerations found in international legal instruments that are relevant for the application of nuclear forensics in response to nuclear security events and analyse how nuclear forensics support the implementation of these measures, thus contributing to strengthen...
nuclear security. It will also address the legal considerations that have to be included in the national legal and regulatory framework to ensure that nuclear forensics serves its primary purpose: provide reliable evidence in the context of legal proceedings under international or national law related to nuclear security.

**State**

Poland

**Gender**

**Primary author:** Ms GIŻOWSKA, Paulina (National Atomic Energy Agency)

**Presenter:** Ms GIŻOWSKA, Paulina (National Atomic Energy Agency)

**Track Classification:** MORC: Nuclear forensics
Regulatory body experience in conducting and using a threat assessment and design basis threat in decision making process for regulating nuclear security

As the threat profile changed rapidly against nuclear and radiological facilities and activities over the last few years, and the emerging of new techniques by terrorist groups in conducting attacks, it becomes crucial to incorporate the threat assessment and design basis threats outcomes in the regulatory requirements for nuclear security for prevention and protection of nuclear and radiological facilities.

The regulatory body depending on prescriptive and performance based approach in regulating nuclear security for those facilities, any how it is very difficult some times to change the regulatory requirements to accommodate the emerging threats against nuclear and radiological facilities, because of those challenges the regulatory body with the support of the national security agencies depend on the threat assessment and the design basis threat to face any emerging threats against the regulated radiological and nuclear facilities respectively.

Further, the purpose of sustainability and ensuring the highest level of protection of nuclear facilities, regulatory body use the design basis threats document as one of the main elements in regulatory inspection and evaluation of nuclear security measures for nuclear facilities, which impact the regulatory evaluation of the physical protection system, security procedures and insider threat mitigation program.

Since the threat changes rapidly in the region, the regulatory body decided jointly with the national security agencies to make the review and assessment process of the design basis threats to be every two years or based on any related trigger events which require an urgent start of the review process of the threat assessment.

There is a lot of benefits from using the threat assessment and the design basis threats outcomes in issuing new or modify the requirements for protection of nuclear facilities, but it comes along with other challenges regarding the need of changing the security measures for those facilities, and there should be an agreement between the regulator and the operator on the required modifications on the security measures to address the targeted threats.

The regulatory body taking into consideration the complexity and the challenges faced the operator that comes from the requirements arise from the periodic review and assessment process of the threats during the decision making process, and for that reason it gives the operator the chance to provide suitable solutions to follow the new requirements without compensation on facility security.

State
Jordan

Gender
Male
Primary author: ALSALMAN, Ahmed (Energy and Minerals Regulatory Commission)
Presenter: ALSALMAN, Ahmed (Energy and Minerals Regulatory Commission)

Track Classification: PP: Design basis threat and threat assessment: prevention and protection
New analytical procedures for the determination of chosen radionuclides by ICP-MS for nuclear forensic purposes.

Nuclear Forensics is defined as the examination of nuclear or other radioactive material, or of evidence that is contaminated (or comingled with) radionuclides, in the context of legal proceedings under international or national laws related to nuclear security [1]. The goal of nuclear material forensics is to establish an unambiguous link between man-made nuclear materials and their intended use, means of processing, point of origin, and routes of transport [2]. Forensic analysis of interdicted nuclear material relies on a wide variety of analytical techniques to establish material provenance, history, and intended use. Taking into account the number of publications on nuclear forensics, which appeared in the last years, it can be concluded that there are still new challenges in this area. The list of analytical techniques which can be used for nuclear material characterization and the obtained corresponding information from each technique is given in [3]. The main goal of this work is to show the possibility of quadrupole ICP-MS (Q-ICP-MS) using for the determinations of isotopic ratios (IR) of U. Usually, for this purpose the high resolution spectrometers are used. Their price is much higher than the standard quadrupole spectrometers, their purchase is not always possible (especially for the developing countries). Radionuclides are present at low concentration levels, so to determine them with high accuracy (to improve the sensitivity and to obtain lower detection limits), the appropriate preconcentration and separation steps should be introduced to the analytical schemes. In this work, using chelating ion-exchangers is proposed.

The studies were partly supported by the IAEA, in the frame of the scientific project: J02013-Applying Nuclear Forensic Science to Respond to a Nuclear Security Event (Contract No. 23061)

State
Poland

Gender
Female

Primary authors: Dr CHAJDUK, Ewelina (Institute of Nuclear Chemistry and Technology); Mr KALBARCZYK, Paweł (Institute of Nuclear Chemistry and Technology); Prof. POLKOWSKA-MOTRENKO, Halina (Institute of Nuclear Chemistry and Technology)

Presenter: Dr CHAJDUK, Ewelina (Institute of Nuclear Chemistry and Technology)

Track Classification: MORC: Nuclear forensics
The Nuclear Forensics International Technical Working Group (ITWG) is a forum for informal technical collaboration among official nuclear forensics practitioners who share a common interest in preventing illicit trafficking of nuclear and radioactive materials out of regulatory control. Together, this community of scientists, law enforcement personnel, and regulators work to advance the best practices of nuclear forensics largely through the participation in a series of Collaborative Materials Exercises (CMX), formerly known as Round Robin exercises, and Galaxy Serpent Exercises (GS).

The ITWG Exercise Task Group (ETG) is responsible for facilitating Collaborative Materials Exercises (CMXs). These exercises are designed as learning experiences rather than performance tests for the scientific community. They utilize well-characterized materials of a known history and origin that are taken from specific process locations within the nuclear fuel cycle. These “real world” materials are used as the basis of exercise materials, as opposed to laboratory-generated pure phase certified reference materials, in order to fully consider the potential significance of process-derived heterogeneities and characteristics suggestive of the material history. While individual laboratory results are held in confidence, a summary of the major outcomes from each exercise are published in the open literature. To date, the ITWG has carried out six Collaborative Materials Exercises with the sixth (CMX-6) and largest (23 participants) recently completed in June 2019.

The ITWG National Nuclear Forensics Libraries Task Group (NNFL TG) is responsible for organizing the Galaxy Serpent (GS) series of exercises, which focus on advancing global understanding of the NNFL concept. There have been three GS exercises to date, all virtual, and designed to give participants experience with methods for organizing material characteristic data, queries a NNFL might receive, and comparative data analysis techniques that might be useful for answering investigative questions. Exercises start by providing material characteristic data to participating teams, followed by two to three rounds of investigative questions the teams are asked to answer based on the results of a hypothetical forensic examination. Example questions included are “how many populations of material are represented in the data set?”, “is a material under examination consistent with any material in the data set?”, and “are two materials under investigation consistent with each other?” Each exercise has focused on a different category of material, including spent nuclear fuel (GSv1), radioactive sources (GSv2), and uranium ore concentrates (GSv3), and each illustrated that the methods for organizing data and the data analysis tools and expertise necessary to answer investigative questions vary depending on material type. Results of the GS exercises have been published in peer-reviewed journals, and are serving as important practical guidance for states looking to establish or advance their NNFL.

State

United Kingdom

Gender

Female
Primary authors: SCHWANTES, Jon (Pacific Northwest National Laboratory); Dr EL-JABY, Ali (Directorate of Security and Safeguards, Canadian Nuclear Safety Commission, Government of Canada); CORBÉY, J. (Los Alamos National Laboratory); LAMONT, Stephen (United States Department of Energy); Ms MARSDEN, Olivia (AWE)

Presenter: SCHWANTES, Jon (Pacific Northwest National Laboratory)

Track Classification: MORC: Nuclear forensics
Phosphate Fertilizer and Nuclear Proliferation – Food for thought

Phosphate fertilizers are produced from phosphate rocks that is one of the most mined materials, by quantity, on this planet. Phosphate rocks can contain considerable amounts of accompanying natural uranium that can exceed concentrations found at commercial uranium mines. Recovering uranium from phosphate rocks during fertilizer production is a technically mature process that was used on an industrial scale in the United States and elsewhere before decreasing uranium prices made this practice unprofitable in the 1990s. Soon, technical improvements, potentially rising uranium prices, and anticipated environmental regulations may make uranium extraction from phosphates profitable again in the United States and emerging phosphate rock mining centers in Northern Africa and the Middle East.

On the one hand, extracting uranium during phosphate fertilizer production is desirable in a way that otherwise lost resources are conserved and fertilizers with reduced radiotoxic heavy metal content are produced. On the other hand, phosphate rocks have also been subject to clandestine uranium acquisition for military programs in the past, and it can be argued that the practice is continued by some state and non-state actors to circumvent sanctions or avoid attention from the international community.

Uranium is found in low to medium concentrations in various materials worldwide. In fact, uranium is considered to be more plentiful than antimony, beryllium, cadmium, gold, mercury, silver, or tungsten and is about as abundant as tin, arsenic or molybdenum. Research on uranium extraction from seawater has a long history and once these technologies succeed to become economically viable uranium will be available to any state on non-state actor with a shoreline.

What makes uranium in phosphate rocks unique are (1) the relatively high concentrations that can exceed those of commercially operating uranium mines, (2) the relatively large quantity of uranium found in phosphate rocks globally that exceed half of the presently known commercial uranium resources and (3) the technical maturity of extracting uranium at commercial scales during wet-phosphoric acid processing for phosphate fertilizer production. The large quantities of phosphoric acid, phosphate rock and phosphate fertilizer traded globally makes imposing controls challenging to say the least and the importance of fertilizers for a countries food security poses equally large challenges on imposing sanctions or otherwise restrict a countries access to phosphate fertilizers.

This work will present a balanced view on the latest discussion about the importance of uranium from phosphates for nuclear proliferation that aims to be the start of a larger international project on this topic.

State

Germany

Gender
**Primary authors:**  HANEKLAUS, Nils (RWTH Aachen University); GEISSLER, Bernhard (Danube-University Krems); STEINER, Gerald (Danube-University Krems); HILTON, Julian (Aleff Group); TULSIDAS, Harikrishnan (United Nations Economic Commission for Europe)

**Presenter:**  HANEKLAUS, Nils (RWTH Aachen University)

**Track Classification:**  PP: Nuclear security of nuclear fuel cycle facilities: emerging technologies and associated challenges and complex threats
NUCLEAR SECURITY CULTURE DEVELOPMENT FOR NEW COMERS

In this paper nuclear security culture development programme (NUSEC) for new comers is presented. NUSEC is the continuation of the safety culture development program designed by NUTEK Inc.

The safety culture development program was created by NUTEK Inc in order to contribute to improve industrial safety and occupational health status in newcomers by building a «safety culture training » along with the «localization activities» starting from the pre-operational phases of NPP projects. During the implementation of the NUSAC one of the main issue was to define and describe clearly the fine line between the safety and security terminology. Both safety and security have the same equivalent meaning in Turkish.

Few years after the initiation of this work, there has been a need to address both safety and security and the interface between the two.

The new module on the Nuclear Security Culture Development Program for new comers reflects the strong interface between safety and security culture issues.

NUSAC (NUTEK SAfety Culture Development Program) Methodology: NUSAC consists of various training modules for introducing and progressively developing human and organizational safety and security culture including evaluation of factors influencing safety culture, risk management, emergency preparedness, risk communication. Safety and security leadership awareness issues are also addressed.

NUSAC has short, medium and long term objectives and will be implemented in accordance with the progress of the current Turkish national NPP projects. NUSAC and new module on the nuclear security stipulates the cooperation with key authorities and stakeholders; ministries, regulatory authority, private sector, industrial chambers, universities and related NGOs and public.

State

Turkey

Gender

Female

Primary author:  Ms GÖKTEPE, Bahire
Presenters:  Ms GÖKTEPE, Bahire;  DAYDAY, Necmi

Track Classification:  CC: Nuclear safety and security interfaces
Challenges for nuclear security of Small Modular Reactors (SMR) in Argentina

The development of different Small Modular Reactor projects around the world will allow the production of electricity in many countries, with benefits in terms of costs, both in the construction and in the maintenance and operation of the facilities, which is a strong incentive for the use of this type of reactors in a wide range of environments and geographical locations.

Currently, the National Atomic Energy Commission (CNEA – Comisión Nacional de Energía Atómica) is developing the CAREM project (Central Argentina de Elementos Modulares), the first power reactor fully designed and built in Argentina, which is a PWR type (Pressurized Water Reactors) with an electrical output of 32 MWe.

Due to the territorial characteristics of a country such as Argentina, CAREM reactors have an important projection for the electrical supply of areas far from the large urban centers, allowing the decentralization of electricity generation as well as the apportionment of the costs associated with the different stages because their modularity (even in case of power increase). Also, these reactors appear as ideal electrical generators for manufacturing centers with high energy consumption, so as to make independent the industrial consumption of the domestic one. In addition, they offer services such as the provision of steam for various industrial uses, or the feeding of seawater desalination plants (facilities that demand high and constant electricity consumption).

The above mentioned cost reduction also implies a simplification in the design of the physical protection system, without compromising nuclear security, which requires to adequate the regulatory approach.

In Argentina, the Nuclear Regulatory Authority (ARN – Autoridad Regulatoria Nuclear) is the entity devoted to the regulation of the nuclear activities in the country, with competence in the areas of radiological and nuclear safety, safeguards and non-proliferation, and physical protection. The ARN is empowered to establish the regulatory standards within its competence, to license facilities and practices that use radioactive material as well as the personnel with safety relevant functions, and to control the activity (performing inspections and regulatory audits).

The objective of this work is to present the current situation in Argentina related to nuclear security for the Small Modular Reactors and the associated difficulty, describing the CAREM project and the applicable regulatory framework, contemplating the challenges represented by the siting, the facility, as well by the transport and storage of the fuel elements. Also, it will be explained the importance of considering nuclear security from an early stage of the design of the project and it will be covered interface aspects between nuclear security and radiological and nuclear safety, elaborating regulatory recommendations with the purpose of establishing nuclear security measures for this type of facilities, in a sustainable manner.

State
Argentina

Gender
Male
Primary authors: Mr ELECHOSA, Christian (Autoridad Regulatoria Nuclear); Mr BOTIGLIERI, Eduardo (Autoridad Regulatoria Nuclear)

Presenter: Mr ELECHOSA, Christian (Autoridad Regulatoria Nuclear)

Track Classification: PP: Nuclear security of new nuclear technologies (e.g., small modular reactors)
Information Fusion Analysis of Cyber Attack Identification Based on D-S Evidence Theory

The control of nuclear power plants (NPPs) is increasingly dependent on digital Instrumentation and Control (I&C) systems. The digitization has brought a series of benefits to the I&C systems of the NPPs, and it also results in a growing and previously unforeseen cyber attack threat. Even if the I&C system adopts preventive measures such as physical isolation, the risk of cyber attack is still unavoidable, which has seriously threatened the safe and stable operation of the power plants.

Cyber attack identification of I&C systems is the first step in cyber attack assessment. Different types of attacks have different impact ranges, urgency, consequences, and countermeasures. Therefore, cyber attack identification is also the basis and premise for correct and real-time attack response.

As the network structure and system functions of the I&C system become more and more complex, the attack methods are also more and more diversified, and the representation of the attack is usually reflected in multiple aspects, which increases the difficulty of cyber attack identification. The attack identification by a single information source is difficult to identify various types of cyber attacks. It is necessary to integrate information from multiple sources through information fusion to obtain more comprehensive and reliable cyber attack identification.

On the other hand, cyber attack information from different sources may have some ambiguity, and even the opposite description. Reasonable collection and screening are needed to fully exploit information, eliminate conflicting information, and focus on mutually validated information to obtain more accurate cyber security awareness.

This paper will use D-S evidence theory to integrate data and information from different sources, including real-time network traffic data, equipment status data, process data, and expert experience data. These data and information will be incorporated into a unified fusion framework and preprocessed in the same format, so that information from different sources can be expressed and interpreted under this framework. The Dempster’s Combination Rule is used to synthesize the basic probability distributions of each evidence, and the Belief function and Plausibility function of each hypothesis are obtained, and the attack type identification is completed.

We will select three typical types of cyber attacks as the objects to be identified, and select the associated multiple measurement for each type of cyber attack as its attributes, which may be shared by different types of attacks. To obtain the basic probability assignment (BPA) of each attribute, it is necessary to solve the multi-attribute decision problem between the cyber attack type and the attributes. This paper intends to adopt the triangular fuzzy number: firstly, the samples of the three attack types are randomly divided into training samples and test samples, then the triangular fuzzy number model on each attribute of the training samples is constructed, and the test samples are matched with the model, and finally the fusion the BPA of each attribute to complete the modeling process.

State

China

Gender
Primary authors: Mr GUO, Chao (Institute of Nuclear and New Energy Technology of Tsinghua University, Beijing 100084, China); LI, Jianghai (Institute of Nuclear and New Energy Technology, Tsinghua University); JIA, Qianqian; ZHOU, Shuqiao; CHEN, Fan; HUANG, Xiaojin

Presenter: Mr GUO, Chao (Institute of Nuclear and New Energy Technology of Tsinghua University, Beijing 100084, China)

Track Classification: CC: Information and computer security considerations for nuclear security
Be wise, exercise - How to prepare your operations and yourself against a nuclear security event

Will you and your team be able to protect against an unpredicted attack? You can assess and test your capabilities by doing exercises.

Protecting against malicious acts by criminals or terrorists is an essential element of global efforts to ensure that nuclear and other radioactive materials, associated activities, and facilities housing them, are kept safe and secure.

Exercises are a key assurance activity supportive of nuclear security. Nuclear Security Fundamentals recognizes that routinely performing security assurance activities is an essential element of nuclear security. Exercises can provide unique insight in the state of preparedness of security. They can also be the basis for continued improvement programmes for all organizations within the State’s nuclear security regime. However, to be most useful, security exercises need to be well organized, professionally conducted and their evaluation must focus on constructive improvement potential.

Exercises is one way to learn about your organizations capabilities. Are you and your organization prepared to tackle the unknown attack? Where is your weak spot? Is it the armed adversaries, cyber attacks, insiders, disruption of communications, a blended attack or some other kind of a nuclear security event that you need to be prepared against?

Do you train your personal and evaluate administrative and technical measures? Which are your requirements for physical protection? Does it reflect a concept of several layers and methods of protection (structural, other technical, personnel and organizational) that have to be overcome or circumvented by an adversary?

Is your preparation enough or do you need to do more?

Exercise is a fantastic tool to plan and prepare yourself and your organization to handle unpredictable situations. It will improve your organizations skills and capabilities and give an understanding of its up’s and down’s. From my long experience I will reveal the magic tools behind a successful exercise, it is all about planing and preparing.

I will explain how you could plan for your and your organizations need. Using my long experience of doing exercises will give you a model on how to answer questions like:

Which type of exercise do I need to do?
Which one gives the best result?
Which tools and manuals can I use?
How do I plan, prepare and conduct an exercise?
What to avoid.

How to do national or international exercises, small ones with a few participants or bigger ones with several hundred participants. Simple ones and complex ones. By adding different languages, culture and traditions gives an even more complexed picture.

In summary I have been doing lots of exercises and also been deeply involved in IAEAs developing of the handbook on Transport Security Exercises and the ongoing work with the handbook regarding Computer Security Exercises.

My presentation will give you the tools and thoughts behind planning of a successful exercise.

The objectives of an exercise may on an organizational level include (but not be limited to):
• awareness (of all personnel)
• training team, decision makers and TSOs
• test the internal procedures and how they are followed
• understanding roles and responsibilities of all, including stakeholders
• testing the communications through chain of command
• continuous collaboration and cooperation between all stakeholders
• justifying the resources for security
• identify gaps in internal procedures and guides, regulations
• understanding the risks
• develop the security culture
• measure overall programme effectiveness
• test the effectiveness of administrative, technical and physical security measures
• test the knowledge and skills of personnel; procedures and knowledge of the procedures (step by step)
• prepare the action plan for improvement of security measures
• lessons learned

Exercise planning with:
- purpose,
- scope,
- objectives,
- target group and limitations,
- exercise types and forms,
- time table for exercises,
- planning organization,
- exercise documentation,
- using IAEA exercise handbooks.

Summary
Exercises are a powerful tool for verifying and improving the quality of computer security arrangements. Each exercise represents a significant investment of effort, financial resources and people. It is therefore important for each exercise to yield the maximum benefit. That benefit depends primarily on the quality of the preparation, conduct and evaluation of the exercise.

State
Other

Gender
Male

Primary author: NIELSEN, Tommy (IAEA)
Presenter: NIELSEN, Tommy (IAEA)

Track Classification: CC: Good practices in the development and execution of nuclear security exercises (e.g. tabletop, drills and field exercises);
AAEA Role in Strengthening Nuclear Security Infrastructure in Arab Countries

The Arab Atomic Energy Agency (AAEA) is a regional specialized organization working within the auspices of the League of Arab States to coordinate among its member states in the field of peaceful uses of atomic energy. It contributes also to the transfer of the peaceful nuclear knowledge and technologies to these countries assist in manpower development and scientific information concerning nuclear sciences and set up harmonized Arab regulations for radiation protection, nuclear safety and security and safe handling of radioactive materials.

As the use of nuclear energy expands in Arab countries and due to the growing concern in the region over the potential of nuclear or radiation accidents, risks of illicit trafficking of radioactive sources and their malicious uses as well as the act of terrorism, the Arab Atomic Energy Agency (AAEA) seeks to enhance the Arab national systems of nuclear security and to create an atmosphere of cooperation and coordination between relevant parties in Arab countries to establish a strong national and regional nuclear security regime. This can be achieved only by collective efforts of Arab countries and international community, AAEA may play a key role in this regard. The AAEA assist to enhance the capabilities and capacity of Arab countries to properly prevent, detect and respond to any potential nuclear security threat by strengthening national infrastructures and exchange the relevant information and knowledge and lessons learned.

A well established, effectively independent, technically competent and efficient regulatory body is considered essential for robust nuclear security. AAEA has established the Arab Network of Nuclear Regulators ANNuR to foster enhancement, strengthening and harmonization of the radiation protection, nuclear safety and security regulatory infrastructure and framework among the members of ANNuR; and to provide mechanisms for the ANNuR to be an effective and efficient internationally recognized forum for the exchange of regulatory experiences and practices among the radiation and nuclear regulatory bodies in Arab countries. ANNuR has 8 thematic working groups one of them about nuclear security. The nuclear security working group has its own action plan including training programmes and technical meetings and get assistance and support from IAEA, KINS, US-NRC, US-DoE, and EU.

The AAEA promotes effective coordination and cooperation among Arab and international organizations to ensure synergies and avoid overlapping in the efforts to establish, maintain and evaluate the national nuclear security systems that will contribute to the global nuclear security regime.

State

Other

Gender

Male

Primary author:  MOSBAH, Daw Saad (Arab Atomic Energy Agency)

Presenter:  MOSBAH, Daw Saad (Arab Atomic Energy Agency)

Track Classification:  CC: Nuclear security culture in practice with a focus on sustainabil-
Argentina has been in a continuous and wide development process in the nuclear activity areas since the 1950s. The use of this strategic resource was assumed as a State Challenge due to its multiple applications to the human beings life style, referred to health and industrial uses including electricity production by Nuclear Power Plants (NPPs).

Nowadays, in Argentina, there are more than 1300 nuclear and radiological installations under regulatory control and the strict compliance of the Argentine Regulatory Standards. The National Nuclear Activity Law 24804, through its Decree Nº 1390, empowered the Nuclear Regulatory Authority of Argentina, (ARN, by its initials in Spanish) with the attribution to develop the corpus of national Regulatory Standards.

The Argentine regulatory framework has been consolidated since the beginning of the nuclear activity with a graded approach. In 1958, it was published the first Standard on the Use of Radioisotopes and Ionizing Radiations, and then, in 1966 it was published the first edition of the Basics Standards on Radiological and Nuclear Safety. Some years later, the standards called "CALIN" applicable to nuclear facilities were issued. Since 1994 the regulatory activity became fully independent with the creation of the National Board of Nuclear Regulations (ENREN, for its initials in Spanish), the predecessor organization of the current Nuclear Regulatory Authority (ARN). The experience on regulatory issues was gained through the application of national regulations which took into account the IAEA standards and the ICRP recommendations. Currently, the Argentine regulatory framework, based on performance Regulatory Standards, covers the regulatory areas of radiological and nuclear safety, safeguards and physical protection of nuclear materials and nuclear facilities, and security of radioactive sources. Nuclear security is one of the main issues considered for the installations and practices regulated by ARN.

In 2016, it was initiated a detailed regulatory framework review to identify gaps in the existing corpus of standards and with the objective of harmonizing the Argentine Standards. The objective of the review was also to contrast the standards with the IAEA Safety Standards recommendations, the mandatory conventions and, in the particular case of security requirements, the Convention on the Physical Protection of Nuclear Material and its Amendment (CPPNM). The standards produced by other recognized regulatory bodies and the experience gained as the result of the licensing and regulatory control of nuclear and radiological facilities were also considered. That resulted in the improvement, updating or extension of the scope of the existing standards and the creation of some new standards.

This paper will present the nuclear security requirements status in the Argentine Regulatory Standards. As a result of this research based on the Regulatory Standards, it was possible to find the connection among the different requirements on nuclear security in the Regulatory Standards. This paper will highlight the updated requirements and explain the necessity of inclusion of some of them in the corpus of the Nuclear Regulatory Standards in order to strengthen the control measures and to foster the nuclear security culture. The clear understanding of the interrelation of the nuclear security requirements in the Regulatory Standards may optimize all the regulatory activities and their associated resources.

State

Argentina
Gender
Female

Primary authors: VALENTINO, Lucia; BOMBEN, Ana Maria; GREGORI, Beatriz
Presenter: VALENTINO, Lucia

Track Classification: CC: National nuclear security regulations
Cyber Security Exercise Georgius 2019

Summary
Executing physical security exercises is common practise at nuclear facilities. Executing cyber security exercises is still less common. In 2019 Urenco Nederland B.V. organised cyber security exercise "Georgius 2019", a multidisciplinary security exercise. The exercise stretched over 3 days and was conducted over in the field. It involved several departments and processes of URENCO Netherlands, as also a range of emergency response and crisis management processes from the public domain. The presentation will explain why this exercises was organised, how it was executed and what the main points were that participants took form this exercise.

Scope of the exercise.
Urenco Nederland B.V. sees doing exercises as essential in ensuring that it’s security measures and the organisation around that are fit for purpose. It gives both the opportunity to train Urenco staff in the right behaviour during unusual and sometimes difficult situations, as that it also demonstrates to Urenco’s General Management and to other stakeholders like the nuclear security regulator that Urenco Nederland B.V.’s security performance is effective to counter the defined threat.

Recently, like in many countries, in the Netherlands there have been made substantial steps in updating cyber security regulation. And not only nuclear facilities themselves, but also emergency response units from the public domain are getting more and more aware that also their effectiveness partly rests on IT support those public emergency response processes need.

This is the core idea behind Georgius 2019, exercising the additional requirements that were made more explicit in recent updates of nuclear security regulation like for instance forensic in the cyber domain as also exercising the impact of a cyber threat (for instance a crypto locker) for emergency response units in the public domain.

Organising the exercise
Organising a multidisciplinary, 3 day long security exercise in the field is a challenge. The presentation will describe what approach was used to bring the different organisations participating in the exercise together and how consensus was reached on what the exercise should do and how it should be organised and conducted.

Executing the exercise
The presentation will also explain how the exercises was executed. So, how the exercise organisers ensured that actions at different locations remained synced in the overall exercises scenario. And it will explain how the evaluation was organised of the exercises which took place on multiple locations in the field.

Lessons learned
And of course the presentation will give an overview of the type of lessons that were learned and will give ideas to maximize the learning effect of other exercises in future.

State
Netherlands

Gender
Male
Primary author: KEIZER, Antonius (URENCO Nederland B.V.)

Presenter: KEIZER, Antonius (URENCO Nederland B.V.)

Track Classification: CC: Information and computer security considerations for nuclear security
Inter-Agency Collaboration in Combating Illicit Trafficking of Radioactive Materials in Kenya

An effective nuclear security infrastructure in a country requires an appropriate integration and coordination of responsibilities among the government agencies. In Kenya, the Radiation Protection Board is the national competent authority on matters of radiation safety, security of radioactive and nuclear materials, control of consumer products contaminated with radioactivity, and other related matters. To effectively carry out these mandate, the Board set up the department of Nuclear Security and Coordination Centre (NSCC). This centre coordinates the activities of other agencies to ensure effective surveillance to combat illicit trafficking of radioactive and nuclear materials in the country and through the border posts. Kenya is strategically located to serve some land locked countries within the East and Central African region. These countries import radioactive sources some of which pass through the Kenyan territory destined for use in industrial and other facilities. This has led to a challenge in tracking the movement of radioactive materials from their points of entry to the end users in other countries. However, through the coordination of agencies, coupled with a robust legislative and regulatory framework, some of the previously identified challenges have been addressed. This paper will give an overview on how these government agencies coordinate in ensuring that illicit trafficking of radioactive and nuclear materials is eliminated in the country. Some of the challenges identified were highlighted and possible solutions recommended.

State
Kenya

Gender
Male

Primary author: ATOGO, Michael (Radiation Protection Board)
Presenter: ATOGO, Michael (Radiation Protection Board)

Track Classification: MORC: Preventing illicit trafficking of nuclear and radioactive material
Evaluation of National Strategies for Regaining Control over Radioactive Material in the United Republic of Tanzania from 2009 to 2018

The safety and security record for the application of nuclear technology in the United Republic of Tanzania is admirable although some incidents involving illegal possession of radioactive material in the country have been intercepted by the national police between 1996 - 2012. Latest incidents of illicit trafficking were recorded in 2009 and 2012. In this matter the safety and security of radioactive sources are very important from the initial stage of the source use to its final disposal stage. The aim of this paper is to evaluate the national strategies for regaining control over radioactive material in the Country from 2009 to 2018. The evaluation covers regulatory framework; education and training of regulatory staff, frontline officers and stakeholders; import/export of radioactive sources; scrap metal industries monitoring; security upgrading of facilities with high risk; management of disused sources; search and secure of orphan sources; radioactive sources inventory; security plan during the transport of radioactive sources; collection and conditioning of disused sources; international cooperation; and implementation of projects and activities Tanzania participated in IAEA from 2009 to 2018.

REFERENCES


State

Tanzania

Gender

Male

Primary authors: SHAO, Didasi W. (Tanzania Atomic Energy Commission); MUHOGORA, Wilbrod (Tanzania Atomic Energy Commission); BUSAGALA, Lazar (Tanzania Atomic Energy Commission); GURISHA, Mikidadi (Tanzania Atomic Energy Commission)

Presenter: SHAO, Didasi W. (Tanzania Atomic Energy Commission)

Track Classification: MORC: Preventing illicit trafficking of nuclear and radioactive material
Physical Protection of Nuclear Materials Issues in Tajikistan 
Ulmas Mirsaidov

Tajikistan has legislation in place which regulates all aspects of the peaceful use of nuclear energy, i.e., radiation protection, safety, physical protection, accounting for and control of nuclear materials and import/export control of strategic goods, including nuclear materials and technology. This legislation provides the basis for Nuclear and Radiation Safety Agency of RT (NRSA) and other State authorities to implement Tajikistan safeguards obligations pursuant to the Comprehensive Safeguards Agreement and the Additional Protocol.

The State System of Accounting and Control of Nuclear Material at State is performing by NRSA, the State nuclear regulatory authority of Tajikistan which is an independent Governmental authority and has the right to elaborate and approve regulations and guidance documents, issue licenses for relevant activities, carry out inspections and independently perform its regulatory decisions. Tajikistan does not have any operational nuclear facility. Eventual reconstruction of the former Argus Research Reactor depends on available financial resources.

Nuclear material is located in the following facilities, nuclear installations and Locations Outside Facilities (LOFs) in Tajikistan and accounted for within the relevant Material Balance Areas (MBAs) and Key Measurement Points (KMPs).

NRSA was established as an independent State nuclear regulatory authority by the Law on radiation protection of 2003. It is responsible for licensing of all activities involving the use of nuclear material. Licenses are issued for a period of 5 or 3 years and can be extended, renewed, cancelled or suspended. Conditions of the license are defined in an attachment to the license.

NRSA elaborates and approves regulations and guidance documents related, inter alia, to accounting for and control of nuclear material and physical protection of nuclear material and facilities.

An "Order of organization of the State systems of accounting for and control of nuclear material and sources of ionizing radiation" approved by the Government Decree No. 499 of October 2013 foresees that an operating organization performs annual physical inventory taking.

Tajikistan was one of the first of the post-Soviet Central Asian States to adopt a law on the State control of export of arms, military equipment and dual-use goods (in 1997).

In Tajikistan provided measures against illicit trafficking of nuclear and radioactive materials and there is presented certain approach in nuclear security issues. During the exploration of nuclear materials more than 500 "orphan" sources were discovered in storages, which were no longer in use or were a legacy from bankrupted companies. Very often managers of newly created enterprises/companies are not aware that such sources exist in the storages under their responsibility.

The joint project of NRSA AS RT and the US Nuclear Regulatory Commission was completed by inventorying and creating a database of radioactive sources. The purpose of this project was to inventory all available of IRS (sealed, open, generators and associated equipment) and create the database of them. Within the framework of this project, the inventory of all sources was completed in all regions of Tajikistan.

All the collected data by sources were entered in the database. This database is called RASOD. The uniqueness of the RASOD program is the automatic determination of current activity and the categorization of sources (the classification is made in accordance with the IAEA and the safety manual - No. RS-G-1.9. - Recommended source categories used in general practice). RASOD is an information system that allows the input, storage and processing of IRS data. RASOD is developed for the regulatory bodies on nuclear and radiation safety.

Physical protection measures had been strengthened at the State Institution of "Radioactive Waste..."
Disposal Site" and at the Tajikistan National University, Scientific Institute. A new central control panel of the physical protection system was installed also at the Republic Oncology Centre. Such upgrades were performed mainly through bilateral projects between NRSA and other States and IAEA.
The physical protection system at the SE Tajikredmet includes a combination of several technical features and guards from armed military forces as well as special services.

**State**
Tajikistan

**Gender**
Male

**Primary author:** MIRSAIDOV, Ulmas (Nuclear and Radiation Safety Agency of Academy of Sciences of the Republic of Tajikistan)

**Presenter:** MIRSAIDOV, Ulmas (Nuclear and Radiation Safety Agency of Academy of Sciences of the Republic of Tajikistan)

**Track Classification:** CC: National nuclear security regulations
CONSEQUENCES OF CYBER-ATTACKS IN A NUCLEAR SECURITY SYSTEM OF A BRAZILIAN NUCLEAR POWER PLANT

CONSEQUENCES OF CYBER-ATTACKS IN A NUCLEAR SECURITY SYSTEM OF A BRAZILIAN NUCLEAR POWER PLANT

João C. B. Fiel1 and Pedro M.R. dos Santos1

1 Instituto Militar de Engenharia (IME)
Praça General Tibúrcio, 80 - Urca
22290-270 Rio de Janeiro, RJ, Brazil
fiel@ime.eb.br

ABSTRACT

This paper aims to describe an assessment of cyber-attacks impacts in the effectiveness of the security system of a hypothetical Brazilian facility that comprises a small modular reactor of iPWR type. Performance data have been extracted from several sources on IAEA. The methodology uses a performance-based approach to calculate baseline system probability of effectiveness (PE) as well as the decrease on PE under the interference of cyber threat. Some attack scenarios are postulated in order to evaluate the influence of this threat in a security project. The scenarios postulated includes credible cyber-attacks in the computational systems that controls exterior, interior, position and fence sensors. Under these simple scenarios, the probability of interruption (PI) of an outsider would decrease to low levels. Consequently, in most of scenarios, even under total probability of neutralization (PN), it would not be possible to mitigate the threat timely, making possible to carry out a blended attack. From the results obtained by this paper, it is possible to easily identify the security level that must be associated to the cyber-systems in the nuclear facility, as indicated by the NSS-17G.

State

Brazil

Gender

Primary authors: BATISTA FIEL, Joao Claudio (Military Institute of Engineering); M.R. DOS SANTOS, Pedro (Instituto Militar de Engenharia)

Presenter: BATISTA FIEL, Joao Claudio (Military Institute of Engineering)

Track Classification: CC: Information and computer security considerations for nuclear security
Scenario Development Through Mapping Transitive Digital Trust Relationships in Computer-based Systems

In 2016 the International Atomic Energy Agency (IAEA) launched a Coordinated Research Project (CRP) on Enhancing Computer Security Incident Analysis at Nuclear Facilities (J02008). One of the major activities undertaken within the CRP was the development of threat scenarios demonstrating the progression of an adversary through the digital systems used within a Nuclear Facility. Another activity undertaken in parallel by the IAEA’s division of Nuclear Security, the development of working material for a non-serialised nuclear security publication to assist member states in conducting Computer Security Exercises for Nuclear Security.

Both activities provoked the question - how best to define a scenario that demonstrates the progression of an adversary through interconnected computer-based systems within a nuclear facility with the goal of creating a compromise that results in nuclear security consequences. The adversary would need to progress through multiple levels of computer-based systems and human operators arranged in and supporting a facilities Defensive Computer Security Architecture (DCSA) to achieve this goal, representing the technical specificities of such an approach was seen as a non-trivial exercise.

This paper will explore a methodology implemented and demonstrated through a software application arising out of the combined discussions of the CRP and development of the Computer Security Exercises for Nuclear Security to articulate such a scenario in a clear, flexible, and concise manner. This methodology is provided from a single philosophy: the foundation of security is trust and the reliance of reprogrammable computer-based systems implies a broadly accepting degrees of imperfect digital trust.

Through treating computer-based systems as another form of trusted insiders the methodology provides for the modelling of scenarios by defining elements (people, information, digital assets, and processes) within and external to a facility. The trust relationships that span a facility can then be defined between each of these elements and then the following rules scenarios can be mapped:

1. Trust is imperfectly applied, there exists trust relationships between some elements and adversaries.
2. Adversaries undertake actions to compromise trust relationships held with a connected element.
3. Once an element itself is compromised it becomes adversarial and the trust relationship it holds in turn can be targeted by an adversaries subsequent actions potentially resulting in further compromise.

Using these simple rules the most advanced computer security scenarios to be expressed effortlessly leveraging multi-disciplinary knowledge held throughout an organisation by reducing the technical specificities typically associated with computer security to a simple question that can be posed to anyone: What do we, and the computers we are responsible for, really trust?

Keywords: IAEA, Computer Security, Instrumentation and Control, Nuclear Facilities, Exercises, Trusted Insider, Software, Scenario

State
Gender

Male

Primary authors:  HEWES, Mitchell (IAEA);  Mr BARRY, Adam;  PETERS, Joshua (Australian Nuclear Science and Technology Organisation);  ESKANDER, Javan (Australian Nuclear Science and Technology Organisation)

Presenter:  Mr BARRY, Adam

Track Classification:  CC: Information and computer security considerations for nuclear security
Beyond the Tank Level: Simulator and Hardware-in-the-Loop Supported Training for Computer Security of Nuclear I&C

In 2016 the International Atomic Energy Agency (IAEA) launched a Coordinated Research Project (CRP) on Enhancing Computer Security Incident Analysis at Nuclear Facilities (J02008). The primary objective of this CRP was to contribute to the improvement of computer security capabilities at nuclear facilities to support the prevention and detection of, and response to, computer security incidents that have the potential to either directly or indirectly contribute to a nuclear security event which adversely affects nuclear safety, nuclear security, or Nuclear Material Accountancy and Control.

The majority of research activities undertaken as part of the CRP were centred around the description, construction, and utilisation of the Asherah Hypothetical Facility. The Asherah facility extends a plant model simulation of a Pressurized Water Reactor with capabilities for hardware-in-the-loop (HIL) and virtualised Operational and Informational technologies to allow the exploration of threat scenarios for training, exercise, and the testing and qualification of defensive computer security measures postulated for use in nuclear facilities.

In parallel to the creation of the Asherah Hypothetical Facility the Division of Nuclear Security’s Information and Computer Security Programme embarked on developing a series of flagship International Training Courses (ITC) to educate participants with a hands-on focused approach to the protection of digital Instrumentation and Control (I&C) systems used in Nuclear Facilities.

The first iteration of the flagship ITCs was run in partnership with the United States of America’s Idaho National Laboratory (INL). As the Asherah hypothetical facility was still in early development the USA ITC utilised a number of exercises running on a mock-up Spent Fuel Pool Cooling (SFPCS). The spent fuel pool cooling system demonstrated a tank level control system able to convey a postulated attack where the water level lowered to a point that heat build-up from decay could no longer be successfully removed from irradiated fuel.

The second iteration of the flagship ITC, will be hosted in partnership with the Korean Institute of Nuclear Accountancy and Control’s (KINAC) International Nuclear Security Academy (INSA). For its capstone exercise INSA will utilise the Asherah Hypothetical Facility providing educators the ability to teach concepts that go beyond a simple tank level system - providing experience to the participants in protecting the diverse set of interconnected and inter-reliant facility functions leveraged in real world nuclear instrumentation and control systems that everyday support, control, and contain nuclear processes. The simulation of the hypothetical facility will be augmented with a hardware in the loop physical mock-up of a condenser and condensate storage system interacting with the simulated plant processes.

This paper through exploration of the participant feedback recorded in both iterations of the flagship ITC will explore the evolution of learning outcomes derived from the use of the Asherah Hypothetical Facility and the provided impact on participant knowledge retention, concept appreciation, and the effect on the ability of the course to deliver on its overarching terminal objective.
Gender

**Primary authors:** HEWES, Mitchell (IAEA); Dr SMITH, Paul (Austrian Institute of Technology); BUSQUIM E SILVA, Rodney Aparecido (Brazilian Government); LI, Jianghai (Institute of Nuclear and New Energy Technology, Tsinghua University); SONG, JAE-GU (Korea Atomic Energy Research Institute)

**Presenter:** HEWES, Mitchell (IAEA)

**Track Classification:** CC: Information and computer security considerations for nuclear security
Coordinating an International Research Project in Computer Security

In 2016 the International Atomic Energy Agency (IAEA) launched a Coordinated Research Project (CRP) on Enhancing Computer Security Incident Analysis at Nuclear Facilities (J02008). The primary objective of this CRP was to contribute to the improvement of computer security capabilities at nuclear facilities to support the prevention and detection of, and response to, computer security incidents that have the potential to either directly or indirectly contribute to a nuclear security event which adversely affects nuclear safety, nuclear security, or Nuclear Material Accountancy and Control. The IAEA received and accepted proposals from seventeen institutes spread across thirteen countries forming one of the largest CRPs that the Division of Nuclear Security had ever undertaken.

The first primary activity undertaken as part of the CRP was the coordinated development Pressurised Water Reactor (PWR) simulation that supported the addition of hardware in the loop (HIL). The simulation allowed simulated plant processes to be replaced by control logic implemented on a PLC or further plant model simulations. Each institute participating in the development of the simulator, known as the builders, was assigned a different reactor subsystem to model through a coordinated process.

The second primary activity was the development and testing of anomaly detection techniques proposed for use within Nuclear Facilities. These activities were delivered by institutes categorized within the project as Capability Providing Organisations (CPOs). A third activity, threat profiling organisations, was designed to support both other activities with scenarios designed to enrich their research processes and outputs.

This paper will explore the process and steps undertaken to come to form a highly functional coordinated team within CRP J02008. In particular it will highlight the methodology used to designate institutes to activities, the difficulties in coordinating teams spread across the range of global time zones, processes used when vulnerability information has been discovered by an institute, and finally software tools used to enhance information exchange, progress tracking, and communications. We hope that our findings will assist future international nuclear security projects to build upon our successes and further iterate a model to coordinate the production and delivery of impactful research results in support of member states.

State

Gender

Male

Primary authors:  HEWES, Mitchell (IAEA); Mr FICHMAN, Bobby; ROWLAND, Michael (Practical Reason Incorporated)

Presenter:  Mr FICHMAN, Bobby
Track Classification: CC: Information and computer security considerations for nuclear security
Established in July 2016, the Tunisian Association of Nuclear Sciences and Awareness is a non-profit association. It aims to raise awareness of the nuclear techniques applications benefits in different domains: energy, health care, environment, agriculture...

Ionizing radiation arising from all these nuclear techniques applications represents a risk to the public even directly or indirectly and it needs to be effectively communicated. Since Tunisia is considered as a new embarking country in nuclear energy, scientists are trying to do their research, they have no time to communicate to the public the benefits, and the risks associated with any applications involving the use of radiation. As a result, the public is afraid when hearing the word "nuclear" and this has an influence on their security. The benefit and the side effect of nuclear techniques applications may not be effectively communicated in a comprehensive, timely and professional manner. In this context, the Tunisian Association of Nuclear Sciences and Awareness addresses the issue of communication of radiation risk and benefits to the public.

While there are different ways of communicating radiation risk, we recognize that certain basic parameters are essential for public awareness. In this context, we are seeking to develop a safety culture before nuclear culture to promote nuclear activities in Tunisia and increase the impact of security by organizing scientific events on nuclear science and technology for peaceful purposes, open days in collaboration with influential partners as well as media information (radio, newspapers ...).

Although the events organized by the Tunisian Association on Nuclear Sciences and Awareness have achieved success for its promotion, public confidence, acquiring the required knowledge of nuclear sciences and techniques. Our association begins to have the trust of the public for the communication related to nuclear and radiological information. To this end, it begins to strengthen the preparedness of Tunisia regarding communication with the public in a nuclear or radiological emergency.

The existing legislative and regulatory Tunisian infrastructure does not meet the needs related to existing and future installations and nuclear facilities. This program was based on the various uses of radioactive sources (mainly medical installations). However, over time the infrastructure is not in accordance with the new standards and international recommendations.

The Tunisian Association of Nuclear Sciences and Awareness is highly motivated to participate in the organization of an informative day addressed to the government decision-makers. This action is needed to sensitize them on the importance of giving priority to the promulgation of the new nuclear law. This event can achieve success when supported by the IAEA.

---

**State**

Tunisia

**Gender**

Female
Security of Radioactive Material and Metal Recycling in the Netherlands

State

Gender

Presenter: Mr VAN XANTEN, Nico
ID 299 Adu Bio

State

Gender