International Conference on Computer Security in the Nuclear World: Security for Safety

Monday, 19 June 2023 - Friday, 23 June 2023

VIC

Scientific Programme

The scientific programme is expected to include original papers guided by the themes listed below.

The first list of themes is divided into general topics to guide the development of papers with further detail provided in the bullets under each theme.

The second list indicates, by theme, specific papers that the Programme Committee identified as suggested topical areas for authors that would address particular concerns associated with each thematic area.

Themes of the conference

Call for papers is arranged according to the following themes for which detailed topics have been listed

State-level strategy and regulatory approaches for computer security in a nuclear security regime

o State-level Strategy on evolving threat and legislative framework on Computer Security
o Computer security regulations and regulatory requirements
o Graded approach to national regulatory requirements for computer security
o Harmonizing regulatory approaches on computer security across a nuclear security regime
o Functions, competencies and effectiveness of competent authorities
o Approaches to coordination among stakeholders involved in information and computer security
o Good practices for notification, reporting and exchange of information between stakeholders on capabilities, infrastructures, requirements (e.g., performance-based or compliance-based), emergency preparedness, incident response…

Computer Security Programme Implementation

o Identification and management of facility functions and adversarial targets within facilities and activities
o Characterization of current and emerging threats, hazards and risks related to computer security for nuclear safety and security
o Practical approaches to risk assessment and to risk management (what is good enough) within a Computer Security program, including risk management framework for nuclear activities and use of Security Operation Centres (SOC)
o Harmonizing approaches to computer security for nuclear security and safety (including emergency preparedness, incident response and forensics)
o Detection, analysis, and response to computer security incidents
o Establishing and maintaining a defensive computer security architecture and/or associated computer security measures, including potential integration of computer security by design

Computer Security in Supply Chain Management

o Ensuring computer security throughout the supply chain
o Managing imbedded digital components/devices security of Original Equipment Manufacturer (OEM)
o Complex supply chain relationship management (suppliers' supplier)
o Risk ownership/management between computer security stakeholders
o System/device/vendor qualifications (performances testing, assessment and certifications, graded approach)
o Practical approaches of supply chain management, including requirements/assessment for

vendors, hardware and software, life cycle management, and dedicated national or industry standards

Practical implementation of Computer Security Assurance Activities

o Conducting computer security assessments for nuclear safety and security
o Preparation, conduct and evaluation of computer security exercises
o Developing and maintaining a computer security training programme
o Organizational procedures and practices to ensure computer security effectiveness
o Measuring computer security compliance and effectiveness: methods and tools for “metrics” of qualitative and quantitative performance measures

Sustainability of Computer Security

o Effectiveness of established approaches for regularly evaluating information and computer security
o Updating regulations to address the changing threat environment
o Safety and computer security interface
o Successes and challenges in digital transition of safety or security related analogue systems
o Lifecycle management of computer security within nuclear facilities and/or functions, including design improvements to mitigate emerging vulnerabilities
o Approaches to measure maturity of computer security programs
o Capability of a nuclear facility or organisation to be risk informed on Computer Security
o Reconciling long term and stable safety process and requirements with evolving digital technologies

Human resources contribution to computer security

o Characterising and resolving challenges in human resources development and retention, including appropriate balance between nuclear and computer security knowledge
o Practical governance of computer security competencies and capabilities in nuclear activities, including team approaches that promote interdisciplinary collaboration and in recognition of intersecting IT/OT disciplines
o Leadership on developing appropriate integration of computer security in the culture of nuclear industry, specifically through education and training
o Assessment and mitigation of insider threat for computer security, including behavioural observation

International cooperation in computer security for a nuclear security regime

o Legally binding and non-legally binding international instruments on information and computer security
o Example of computer security guidance and standards relevant in nuclear safety and security (e.g. International Atomic Energy Agency (IAEA), International Organizations for Standardization (ISO), International Electrotechnical Commission (IEC))
o Raising awareness among international organizations, industry, civil society, and other stakeholders about computer security
o International cooperation and assistance to enhance computer security

Computer security of emerging digital technologies for nuclear activities

o Impact and/or application of smart devices, automation tools, digital twins modelling, Artificial Intelligence (AI)/Machine Learning (ML), Information Technology (IT)/Operation Technology (OT) convergence, cloud computing, Internet of Thing (IoT), Block Chain, Quantum computing, etc.
o Computer security considerations for new reactors designs (Small Modular Reactors, Micro Reactors, etc.)
o Computer Security modelling and simulation activities
o Effect of new working environment (e.g. Mobility) for employees/contractors on computer security

Suggested Papers of major interest

Programme Committee established key potential computer security concerns for States that would be particularly interesting to encourage the production of papers that could be focused on.

State-level strategy and regulatory approaches for computer security

Potential concerns: The State's strategy, regulation and DBT for computer security cannot maintain pace with and reflect the rapidly changing nature of the technology and of the consequent threats. Even if the State's requirements change faster, the operator cannot keep pace.
The relationship between state, regulator and operator for computer security is hard to express in a DBT leading to a lack of clarity over the State role and the operator role.
Paper: A member state case study describing how it has dealt with the practical issues regarding DBTs for computer security.

Potential concerns: Computer security is not positioned at a sufficient level of seniority and priority within some organisations because risks are not understood. Safety is generally recognised as a board-level issue while security is frequently delegated to a more junior level. Consequently, security culture is significantly weaker than safety culture; security can have inadequate programme management.
Paper: A member state case study that shows how these issues have been or are currently being addressed.

Potential concerns: Some organisations lack the necessary computer security competence to perform the tasks expected of them, specifically lacking practical understanding of computer security risk management.
Paper: A case study of how member states are addressing the lack of computer security competence.

Computer Security Programme Implementation

Potential concern: Some systems engineering is insufficiently mature to include computer security or produce a coherent defensive computer security architecture. The different disciplines (including security, safety) work in silos despite their interdependencies.
Paper: A member state case study showing Cyber Informed Engineering, security by design, STPA and related approaches to show how practical engineering processes can accommodate computer security throughout the entire lifecycle.

Potential concern: Defensive computer security architectures must recognise that connections of OT to IT business systems and vendors are necessary, while managing the risks to an acceptable level.

Paper: A member state case study describing practical approaches to this issue of external connectivity and how to assure what is entering and leaving.
Paper: A member state case study about a set of architectural design principles for designers, like the IAEA idea of DCSA requirements with a Graded Approach and DiD.

Potential concern: IT and OT are often managed in separate silos but need more sophisticated relationships because of their increasingly complicated interfaces and technology convergence. “Joint-working” or “multi-disciplinary working” are important characteristics. Understanding what information the facility possesses and where it can be found is vital.

Paper: A member state case study that describes the blurred interface between OT and IT, illustrating the synchronisation and collaboration needed between the different teams e.g. for patching, network management, incident response.

Potential concern: There is a mismatch in the anticipated lifetime of the assets of an NPP and the lifetime of the I&C systems based on digital technology.

Paper: A member state case paper about anticipating the obsolescence of the digital technology upon which I&C systems are based.

Potential concern: The interdependencies between safety and computer security is made more significant by digital technology but the two disciplines continue to operate in their own silos, within the operator and the regulator.
Paper: A case study from a regulator showing how its teams work together while maintaining separate teams’ identities, resolving conflicts such that neither discipline should completely override the other and the disciplines are complementary.

Potential concern: The interdependencies between safety and computer security is made more significant by digital technology but the two disciplines continue to operate in their own silos, within the operator and the regulator.
Paper: A member state case study e.g. showing how PPS personnel collaborate with computer security personnel to harden PPS and how PPS protects digital assets.

Potential concern: Information security and computer security interdependencies are increasing due to the use of digital technology but standards and guidance do not adequately reflect this.
Paper: A member state case study or an academic paper that identifies the key differences in computer security controls between those that are appropriate for I&C systems vs. an IT environment.

Computer Security in Supply Chain Management

Potential concern: Current approaches to computer security in the supply chain do not address all the risks, can be too focused on the certification of products and rely too much on stating computer security requirements in contract terms.
Paper: Current approaches to computer security in the supply chain do not address all the risks, can be too focused on the certification of products and rely too much on stating computer security requirements in contract terms.
Paper: A member state case study about the impact of Solar Winds or Log4J and what lessons were learned.

Potential concern: Computer security risks of contracts are frequently not actively managed for the entire period of the contract.
A **Paper** that identifies some best practice in contract award, integration of deliverables and assessment of performance to maintain computer security.
A **Paper** that describes technical and contract teams work together to manage computer security risks in the supply chain.

Potential concern: Some contract acquirers place unwarranted trust in the activities of their suppliers because, for example, there is insufficient assurance of the products and services from lower tier suppliers.
A **Paper** about the use of test and reference environments to perform component and system testing before deploying to a live environment, including the computer security measures needed for that environment.

Human resources contribution to information and computer security

Potential concern: Organisations cannot attract, train and retain staff with the right knowledge, skills and competencies for computer security.
This may be about money but it can also be about career paths with training to maintain technical skills, feeling valued and understood with a place in the organisation.
Paper: A member state paper on its strategy to develop its computer security workforce for OT / I&C.

A **paper** about a computer security competency framework that covers OT / I&C systems and how it contrasts with IT.
A member state **Paper** or case study on establishing a national training programme / centre of excellence that covers computer security for OT / I&C.

Potential concern: A lack of awareness by staff can lead to simple mistakes with serious consequences.
A **paper** describing how security culture can become more like safety culture in the way that people accept its importance as part of daily activities, how security training must be taken seriously and time devoted to it by the business.

Potential concern: A lack of awareness by staff can lead to simple mistakes with serious consequences when staff are working from home.
A **paper**about a successful awareness programme about the issues of home working, particularly lessons learned during Covid lock-down conditions.

Potential concern: A lack of understanding of the insider threat can lead to unseen vulnerabilities.
A **paper** about successful policies to address insiders including those who have malicious intent and those who are unwitting, those who are manipulated or those who act through ignorance or careless acts.

Computer security of emerging digital technologies

Potential concern: Sensors and actuators are being manufactured with embedded networked digital technology, whether required or not. Though user may have the option of disabling the additional features, some don’t realise.
Paper: A member state case study about “smart” sensors and actuators, about the issues and the

procedures to detect their unwitting use or to test and verify that they can be rendered “dumb”.

Potential concern: Smart devices can represent a risk and an opportunity for computer security but standards and guidance may not reflect either the risks or the opportunities. Rules may seek to avoid all risks with a blanket prohibition that get the balance wrong.
Paper: A member state case study about getting the balance right between the issues and opportunities arising from new technology such as might arise with SMR designs.

Potential concern: Suppliers and vendors are recommending increasing use of remote-monitoring and remote-control of some systems as measures to improve efficiency. These connections go outside the traditional boundary of the facility and must be managed very carefully.
Paper: A case study about SMR/MRs use of remote-monitoring and –control for economic reasons, how to assure safe operation against malicious action.

International cooperation in information and computer security for nuclear security

Potential concern: Some states may be reluctant to co-operate with neighbours, in operational timescales, on computer security incidents because of the sensitivity of cyber-attacks in nuclear and non-nuclear sectors. Those states are unable to ask for advice and support or learn best practices and processes from neighbouring states.

A **paper** describing a success story involving States' cooperation

Assurance

Potential concern: Penetration testing of I&C systems is potentially dangerous if performed without appropriate care. However, some organisations prohibit pen-testing completely and have inadequate alternatives to provide assurance.
Academic **paper** or a member state case study that vulnerability assessment, penetration testing and other forms of assurance testing in OT environments cannot be performed in the same way as in IT environments. However, OT penetration testing can be done with the right approach e.g. offline unit testing, using digital twins.

Potential concern: Suppliers and vendors may want to use machine-learning algorithms in newer I&C systems but there is inadequate assurance of the data sets or the algorithms. There are no standards to follow.
Paper: Member state case study showing how machine learning (ML) may be used in a supporting role for I&C systems, e.g. decision support. ML is already being used in computer security tools, for IT and for OT.

Sustainability including security monitoring and incident response

Potential concern: How to model threats and anticipate adversary activities in I&C environments
Paper: A member state case study describing practical models for threat modelling.

Potential concern: How to provide real-time monitoring and security operating centres for OT.
Paper: A member state paper describing practical experiences in setting up real-time monitoring and an OT SOC to cover I&C: who does it, where it is located, how to categorise and prioritise computer security incidents.

Potential concern: How a computer security incident response (IR) programme gets designed, evaluated, exercised, assessed and operated for I&C systems, also covering cover recovery.
A member state **paper** on incident response and how this gets integrated (and vice versa) into the wider IR / Emergency Response / Crisis Management Plan process for the facility and the state.

Potential concern: How to operate in the event of a loss of power and in particular how to ensure that there is no loss of essential data – its confidentiality, integrity and availability.
A member state **paper** about the design and implementation of a data recovery plan, describing how IT and OT environments are restored to a known good state.

Potential concern: How to prepare for and then perform computer security forensics on I&C systems.
Paper: A member state case study or an academic paper on computer security forensics.