Abstract No. 596 - Cross-cutting/Overarching topics - National nuclear security regulations

Overview of Nuclear Cyber Security Requirements for Nuclear Power Plants (NPPs)

Arinze, U.C.[1], Eneh, A.H.[2], Longe, B.O.[3]

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, encipherment, defence-in-depth (DID), design basis threat (DBT), IAEA technical guidance documents such as: GS-R-1, GS-R-2, GS-R-3, GS-G-3.1-3.5, NSS20, NSS23-G, 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 a regulatory perspective on nuclear cyber security, its relationship to nuclear safety and security, 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

[1]Information and Communication Technology (ICT) Unit, Department of Radiological Safety,
Nigerian Nuclear Regulatory Authority (NNRA), South East Zonal Office, Enugu, Enugu State.
[2]Computer Science Department, Faculty of Physical Sciences, University of Nigeria, Nsukka (UNN), Enugu.
[3]Department of Information Systems, School of Information Technology & Computing,
American University of Nigeria (AUN), Yola, Adamawa State.
***Email**: [1]uchechukwu.arinze@nnra.gov.ng, [2]agozie.eneh@unn.edu.ng, [3]olumide.longe@aun.edu.ng*
***Tel**: +2348066532557, +2348076756975, +2348160900893*

1. Introduction

Cyber security includes all processes and mechanisms by which any digital equipment, information or service is protected from unintended or unauthorized access, change or destruction. As a component of nuclear security and the design basis threat (DBT) [1], cyber security is the range of measures enacted to prevent, detect, or respond to the theft of Category I nuclear material or to the sabotage of a nuclear facility, which could result in catastrophic radiological consequences by either exploiting vulnerabilities in information and computer systems alone or combined with physical attacks [2]. According to the United States Nuclear Regulatory Commission (U.S. NRC) Regulatory Guide (RG) 5.71, cyber attack is the manifestation of either physical or logical (i.e., electronic or digital) threats against computers, communication systems, or networks that may originate from either inside or outside the licensee's facility, have internal and external components, involve physical or logical threats, be directed or non directed in nature, be conducted by threat agents having either malicious or non-malicious intent and have the potential to result in direct or indirect adverse effects or consequences to critical digital assets (CDAs) or critical systems (CSs). This includes attempts to gain unauthorized access to a CDA and/or CS's services, resources, or information, the attempt to compromise a CDA and/or CSs Integrity, Availability, or Confidentiality (C.I.A triad) or the attempt to cause an adverse impact to a Safety, Security and Emergency Preparedness (SSEP) functions.

The importance of this paper is underscored by the fact that nuclear security is tremendously impacted by cyber security. Nuclear facilities made up of field devices, field controllers, supervisory control and data acquisition (SCADA) and instrumentation and control (I&C) systems as shown in Figure 1 are mission-critical infrastructure that are susceptible to attacks from Nation States and non-state actors like hactivist/hactivism, third-parties, organised crime, professional criminals, spies, voyeurs, corporate raiders, disgruntled insiders, vandals, script kiddies and cyber terrorists. The various threat actors have different motivations, intentions for their activities, and capabilities, which adds to the complexity of the problem and increases the need for comprehensive understanding of the risks at regional, industry, institutional and process levels.

In May 2018, there were 450 nuclear power plants (NPPs) in operation around the world, generating 393, 836 MW(e) total out of which 195 units (43.3%) were built in the last 30 years and 319 units (70.8%) were constructed during the last 25 years. Currently there are 439 operational nuclear reactors net installed capacity across 31 countries according to the International Atomic Energy Agency (IAEA) Power Reactor Information System (PRIS) database. These critical facilities use both analog and digital systems to monitor and operate plant processes, equipment, and store and retrieve information. In addition to physical and system operational security, cyber security of CDAs and computer instrumentation and control systems (ICS), networks have become a growing concern to both nuclear operators and nuclear facility regulators around the world. I&C components such as process control systems (PCS), supervisory control and data acquisition (SCADA), digital control systems (DCS) that interconnect plant systems performing safety, security, and emergency preparedness (SSEP) functions are not isolated from the Internet. This presents an attack vector for cyber threats.

2. Analysis of Model Frameworks and Standards

This section provides detailed overview of cyber security Standards, Frameworks and Requirement specifications for addressing security vulnerabilities in IT/ICS systems used in NPPs. Cyber security Standards are set of specifications for the cyber security of I&C systems used in NPPs. A Framework is a risk-based approach to reducing cyber security risk. It comprises of three (3) parts: the Framework Core, the Framework Implementation Tiers and the Framework Profile [31] as shown in Figure 2.1.

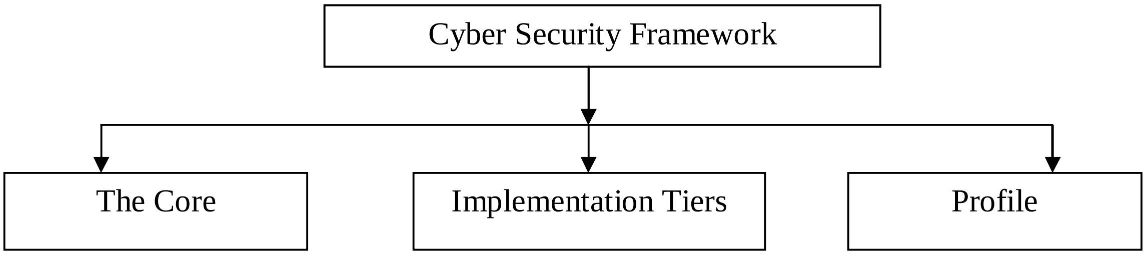

Figure 2.1: Cyber security Framework structure

The Framework Core is a set of cybersecurity activities and references that are common across critical infrastructure sectors and are organized around particular outcomes. It comprises of four (4) types of elements: Functions, Categories, Sub-categories, and Informative References. The Framework Implementation Tier is a lens through which to view the characteristics of an organization's approach to risk - how an organization views cyber security risk and the processes in place to manage that risk. The Framework Profile is a representation of the outcomes that a particular system or organization has selected from the Framework Categories and Sub-Categories [31].

The selection of a framework should be informed by baseline assessment, risk appetite and governance model. The primary consideration to be made by those with accountability for cyber security of nuclear facilities is ensuring that when implementing a framework, linkages and integration are created with the governance model, risk appetite, strategic plan and the broader enterprise risk management functions. It is also important to consider the broader regulatory framework and environment to inform framework selection. These nuclear cyber security frameworks are categorized into IAEA and country-specific frameworks. The lists of nuclear cyber security frameworks, requirements, guidance are provided in Tables 2.1-2.3, while Table 2.4 highlights the comparative analysis of the main requirements of IAEA Draft, U.S NRC RG 5.71 and IEC 62645 CDI.

Table 2.1: IAEA Nuclear Computer/Cyber Security Requirement Sources

S.No.	Title of Publication	Type	Summary
1	**IAEA Nuclear Security Series Number 20 (NSS 20): Objective and Essential Elements of a State's Nuclear Security Regime, 2013.**	Fundamentals	Provide for the establishment of regulations and requirements for protecting the confidentiality of sensitive information and sensitive information assets.
2.	**IAEA NSS 13: Nuclear Security Recommendations on Physical Protection of**	Recommendation	Provides a set of recommended requirements to achieve the

	Nuclear Material and Nuclear Facilities (INFCIRC/225/Rev 5), 2005.		four Physical Protection Objectives and to apply the 12 Fundamental Principles. Section 4.10 states: "Computer-based systems used for - physical protection, nuclear safety, and nuclear material accountancy and control should be protected against compromise (e.g. cyber attack, manipulation or falsification) consistent with the the threat assessment or DBT."
3.	**IAEA NSS No. 17: Computer Security at Nuclear Facilities, 2011.**	Technical Guidance	Provide guidelines to personnel designing, implementing, and managing I&C and information systems (IS) and networks at nuclear facilities. It addresses prevention and detection of potential attacks through reference to best practices in architecture, assurance and management of security information and I&C systems.
4.	**IAEA NSS No. 23-G: Security of Nuclear Information**	Technical Guidance	Provides guidance on implementing the principle of confidentiality and on the broader aspects of information security (i.e. integrity and availability). It specifically seeks to assist Member States in the identification, classification, and assignment of appropriate security controls to information that could adversely impact nuclear security if compromised.
5.	**IAEA Defence in Depth in Nuclear Safety (INSAG 10), 1996.**	Implementing Guide	Provide NPPs with DID implementing guidelines. Outlines five (5) levels of DID that should be sustained at NPPs.
6.	**IAEA NSS No. 33-T: Computer Security of Instrumentation and Control Systems at Nuclear Facilities, 2018.**	Technical Guidance	Provides guidance for the protection of I&C systems at nuclear facilities on computer security against malicious acts that could prevent such systems from performing their SSEP functions. Its scope include: application of computer security measures to I&C systems, application of such measures to the development, simulation and maintenance environments of these systems.
7.	**IAEA Computer Security for Nuclear Security (NST045), 2016.**	Implementing Guide (Under development)	Provide guidance on developing, implementing and integrating computer security as key component of nuclear security. Applies to the computer security aspects of nuclear security regime.
8.	**IAEA Computer Security Techniques for**	Technical Guidance	Provides discussion on good

	Nuclear Facilities (NST047).	Under development)	practices for implementing computer security associated digital technologies at nuclear facilities.
9.	**IAEA Computer Security of I&C Systems at Nuclear Facilities (NST036), 2016.**	Technical Guidance	Provides guidance on implementing computer security controls across the life cycle of nuclear I&C and control systems.
10.	**IAEA Conducting Computer Security Assessments (NST037), 2015.**	TECDOC Series	Provides good practices for organizing and conducting computer security assessments associated with nuclear security.
11.	**IAEA Computer Security Incident Response (NST038), 2015.**	TECDOC Series	Provides good practices for implementing computer security incident response processes between competent authorities, operators, and technical support organizations.
12.	**IAEA Computer Security during the Lifetime of a Nuclear Facility (NST051), 2016.**	Technical Guidance	Provide guidance to States, competent Authorities and operators on appropriate nuclear security measures during the different stages in the lifetime of a nuclear facility. Covers nuclear safety, security and safeguards.

Table 2.2: International Standards Organizations Cyber Security Requirement Sources

S.No.	**Title of Publication**	**Type**	**Summary**
1.	**IEEE 7-4.3.2-2016: Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations, 2016.**	Standard	This standard serves to amplify criteria to IEEE Std 603(TM)-2009, to address the use of programmable digital devices as part of safety systems in nuclear power generating stations. The criteria contained herein, in conjunction with criteria in IEEE Std 603-2009, establish minimum functional and design requirements for programmable digital devices used as components of safety systems.
2.	**IEEE 1686-2013: Standard for Intelligent Electronic Devices (IEDs) Cyber Security Capabilities, 2008.**	Reference	The standard defines functions and features to be provided in intelligent electronic devices (IEDs) to accommodate cybersecurity programs. It addresses security regarding the access, operation, configuration, firmware revision and data retrieval from an IED. Confidentiality, integrity and availability of external interface of the IED is also addressed.
3.	**IEC 61513: Nuclear Power Plant - Implementation and Control Important to Safety General Requirements for Systems, 2011.**	Standard	Provides requirements and recommendations for the overall I&C architecture which may contain either or both technologies. The main technical changes are: alignment with the latest revisions of IAEA documents, alignment with the new editions of IEC 60880, IEC 61226, IEC 62138, IEC 62340, IEC 60987, alignment with significant advances of software engineering techniques and integration of requirements for staff training.
4.	**ISO/IEC TR 13335-1: Information Technology -**	Standard	Provide a standard for IT security. Consists of

	Guidelines for the Management of Information Technology Security, 2001.		Five (5) parts: Concepts & models for managing & planning IT Security, Techniques for the Management of IT Security, Selection of safeguards & Management guidance on Network Security.
5.	**ISO/IEC 27000:2009** **ISO/IEC 27001:2005** **ISO/IEC 27002:2005** **ISO/IEC 27005:2008** **ISO/IEC 27006:2007**	Standard	Developed from BS7799 published in the mid-1990. The British Standard accepted by ISO/IEC as ISO/IEC 17799:2000 revised in 2005 and re-numbered in 2007 to align with other ISO/IEC 2700 series standards. It provides best practice recommendation on information security management for use by those with accountabilities for initiating, designing, maintaining information security management systems.

Table 2.3: Country-Specific Cyber Security Requirement Sources

S.No.	Title of Publication	Country	Type	Summary
1.	**NIST Special Publication 800-82 Rev 2: Guide to Industrial Control Systems (ICS) Security, 2014.**	U.S	Standard	Provide guidance for securing ICS, including SCADA, DCS and other systems performing control functions. Outlines notional overview of ICS, reviews typical system topologies and architectures, identifies known threats and vulnerabilities to these systems etc.
2.	**NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems, 2002.**	U.S	Reference	Provide guidance for conducting risk assessments of Federal Information Systems and organizations, simplifying the guidance in SP 800-39. It satisfies the requirement of FISMA.
3.	**NIST Special Publication SP 800-53A Rev 1: Guide for Assessing the Security Controls in Federal Information Systems in Organizations, 2008.**	U.S	Reference	Provides guidelines for developing security assessment plans and associated security control assessment procedures that are consistent with SP 800-53, Revision 3 in all phases of the development life cycle.
4.	**NIST Special Publication 800-53 Rev 3: Recommended Security Controls for Federal Information Systems and Organizations, 2009.**	U.S	Reference	This standard supersedes NIST SP 800-53A Rev 1. It provides a set of security controls that can satisfy the breadth and depth of security requirements levied on information systems and organizations and that is consistent with and complementary to other established information security standards.
5.	**NIST FIPS PUB 140-2: Security Requirements for Cryptographic Modules, 2002.**	U.S	Reference	Is a Computer Security Standard used to approve cryptographic modules that include both software and hardware components. An initial publication was on May 25, 2001 and was last updated December 3, 2002.
6.	**NEI 04-04 Rev 1/NEI 08-09 Rev 6: Cyber Security Program for Power Reactors, 2005/2010**	U.S	Rule	Provides a template for nuclear power reactor licensees with a means for developing and maintaining a cyber security program at their sites. The plan includes a defensive strategy that consists of a defensive architecture and a set of security controls that are based on NIST SP 800-82, Final Public Draft, Dated September 29, 2008, "Guide to ICS," and NIST SP 800-53, Revision 2, Recommended.
7.	**NEI 10-04 Rev 2: Identifying Systems and Assets Subject to the Cyber Security Rules, 2012.**	U.S	Rule	Provide guidance on the identification of digital computer and communication systems & networks subject to the requirements of 10 CFR 73.54. Utilizes the licensee's Current

				Licensing Basis (CLB) to ascertain important-to-safety functions in the context of the NRC Cyber Security Rule.
8.	**Nuclear Regulatory Commission (N.R.C) Regulatory Guide (RG) 5.71: Cyber Security Programs for Nuclear Facilities, 2010.**	U.S	Regulatory Guide	Provides comprehensive guidance to applicants and licensees on satisfying the requirements of 10 CFR 73.54 that the OMB approved under OMB control number 3150-002 by using NIST SP 800-53, Rev 3 framework.
9.	**N.R.C Regulatory Guide (RG) 73.54: Protection of Digital Computer and Communication Systems and Networks**	U.S	Reference	Performance-based programmatic requirement that ensures that the functions of digital computers, communication systems, and networks associated with SSEP functions are protected from cyber-attacks. Licensees provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design-basis threat (DBT), as described in 10 CFR 73.1, "Purpose and Scope".
10.	**N.R.C Regulatory Guide 5.83 (RG 5.83): Cyber Security Event Notifications, 2015.**	U.S	Rule	Addresses cyber security event notification requirements. Describes approaches and methodologies that staff of the U.S. N.R.C considers acceptable for use by NPP licensees when categorising certain cyber security event, and the process for conducting notifications and submitting written security follow-up reports to the NRC for cyber security events.
11.	**N.R.C Regulatory Guide (RG) 1.152 Rev 2 & 3: Criteria for Use of Computer in Safety Systems of Nuclear Power Plants, 2006. (U.S.)**	U.S	Rule	Provided specific guidance to nuclear power plant licensees for use in the design, development and implementation of IT/ICS systems.
12.	**Template for the Cyber Security Plan Implementation Schedule**	U.S	Rule	Provides a template used by each operating power plant to establish the schedule for the implementation of their cyber security plans.
13.	**Department of Homeland Security (D.H.S) Catalog of Control Systems Security: Recommendations for Standards Developers, 2009.**	U.S	Reference	The catalog presents a compilation of practices that various industry bodies have recommended to increase the security of control systems from both physical and cyber attacks.
14.	**D.H.S Cyber Security Procurement Language for Control Systems, Version 1.8, 2008.**	U.S	Reference	Summarize security principles that should be considered when designing and procuring control systems products (software, systems, and networks) and provide example language to incorporate into procurement specifications.
15.	**D.H.S Cyber Security Assessments of Industrial Control System, 2017.**	U.S	Reference	Covers the process of planning an ICS cyber security assessment, including how to select testing areas and reporting process.
16.	**D.H.S Recommended Practice for Patch Management of Control Systems, 2008**	U.S	Reference	The report recommends patch management practices for consideration and deployment by ICS asset owners. It specifically identifies issues and recommends practices for ICS patch management in order to strengthen overall ICS security.
17.	**D.H.S Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-in-Depth (DID) Strategies**	U.S	Reference	The report provides guidance for developing defense-in-depth strategies for organizations that use control systems networks while maintaining multi-tier information

				architectures.
18.	**Regulatory Document (REGDOC) - 2.5.1: Design of Reactor Facilities - Nuclear Power Plants, 2014.**	Canada	Regulatory Guide	Provides overall status of Canadian regulatory framework for cyber security, as well as key requirements of new CSA standard N290.7-14. Cyber Security aspects of Computer-based I&C systems.
19.	**Korea Institute of Nuclear Safety Regulatory Guide - KINS/RG N08.22: Cyber Security for I&C System, 2009. (South Korea)**	Republic of Korea	Regulatory Guide	Provides a framework for guidance in implementing cyber security controls at Korean NPPs.

Table 2.4: Comparative analysis of the main requirements of IAEA Draft, U.S NRC RG 5.71 and IEC 62645 CDI [32]

Document Categories	**IAEA Draft (66 pages)**	**U.S NRC RG 5.71 (105 pages)**	**IEC 62645 CDI (37 pages)**
Main entity and definition	Computer security (synonym of cyber security) is a particular aspect of information security related to computer based systems, networks and digital systems. Information security - the security of any information regardless of the media used to store or transmit the information. Includes the preservation of the confidentiality, integrity and availability attributes of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.	There is no security definitions Cyber security - protection against cyber attacks is meant.	No security definitions Computer security - reference to IAEA guidance The goal of the computer-based security is to protect the I&C systems from deliberate and intelligent attacks that may jeopardise overall plant safety and availability.
Security Control	Personnel security, Physical security, Nuclear security (in 1.2.1, not in Glossary) Management systems, Organizational issues, Implementing computer security.	Technical, Operational and Management control	11 security categories and Security Programme management.
Related documents	Site Security Plan Computer Security Plan (can be a part of SSP)	Cyber Security Plan Cyber Security Program	Security Programme Computer Security Plan
Requirements to vendors	It is paramount that the security department works closely with the contracts department to ensure that the security provisions are incorporated in each contract. When considered necessary, checks and audits should be made to ensure that the contracting organization's management system adequately addresses security issues, and that the organization's practices and measures are in compliance	There are no direct requirements, only from utility point of view	There are no direct requirements. Platform and application security is a part of operational security procedures.

	with the system.		
Life cycle	Security management lifecycle (spiral shape)	Security lifecycle process (spiral shape)	Linear Life Cycle Implementation of Computer Security
Levels of security	Five levels of security (strength of measures)	Five levels of cyber security defensive architecture	Five levels of computer security protective measures

3. Lessons Learned

The various cyber security incidents reported in this paper and vulnerabilities of I&Cs deployed in NPPs around the world hold important lessons for the cyber security of nuclear facilities and critical digital infrastructure in general.

a. The notion of air-gap separating control and protection sections of NPPs has been proved wrong. The case of Davis-Besse NPP shows that this is a misconception. Operators who try to monitor and protect every connection cannot be sure they know about all of them. Stuxnet was transmitted via thumb drives to infect computers that were not connected to the internet.

b. Security vulnerabilities as a result of digital I&C deployment across CDAs are more complicated than earlier thought by alarmists and sceptics.

c. The various cyber security incidents reveal that Process Control Systems (PCSs) are not immune from attacks since they are different from ordinary computers as widely believed.

d. There is need for an understanding of current cyber security challenges and threat. NPPs responsible for power generation, enrichment and storage are complex computing environments consisting of hundreds to thousands of individual devices. These devices and computer systems that manage them are built from a combination of common, off-the-shell (OTS) computing technologies and custom, one-of-a-kind hardware, software and networking protocols. The only commonality between these facilities is that a large number of their critical systems tend to be built on legacy technologies. The current ad hoc approach to computer security that attempt to detect and block cyber-attacks using intrusion detection systems (IDS) is attack-centric and needs to change to a proactive, risk based approach.

e. Due to dynamic and complex threat landscape confronting computer systems deployed at NPPs, a new approach to computer security is needed, centered on sound principles and technologies that can be used to construct effective defenses. The vulnerability-centric security approach seeks to address the root cause of system insecurity - system vulnerabilities - and creates the opportunity for security to be more constructive.

4. Summary and Conclusion

From this study, only three out of the five countries possess written cyber regulations (U.S.A, Germany and Russia); China and South Africa do not have these regulations. The diversity in the ways in which cyber capabilities can be used poses one of the greatest challenges in Information technology. Computer security must be an essential component in an effective and robust nuclear security regime, so as to guard against increasingly sophisticated cyber threats in a digitally-dependent environment. Nonetheless, particularly the computers used in safety and safety-related systems must be very well protected from possible intrusions. But other computers must be protected as well. The computers used to control the plant are essential to assure the continuity of power production. The computers used to control access to sensitive areas are needed both to prevent unauthorized access that might be part of an attack, and to assure authorized access both for safety and security reasons. Computers that store important and sensitive data have to be protected to assure that those data are not erased or stolen. Possible cyber attacks could be associated with business espionage, technology theft, a disgruntled employee, a recreational hacker, a cyber activist, organized crime, a nation state, or a terrorist organization.

References

[1]Haney, C. (2013). Cyber Security, Office of Nuclear Material Safety, United States Nuclear Regulatory Commission (U.S.N.R.C).

[2]Gluschke, G. et al. (2015). Cyber Security at Nuclear Facilities: National Approaches. An Institute for Strategic Studies (ISS), Brandenburg University of Applied Sciences, Institute for Security and Safety research project in cooperation with the Nuclear Threat Initiative (NTI), U.S.A.

[3]Abadi and Needham, (1996). Prudent engineering practice for cryptographic protocols. IEEE Trans. Software Engineering *Vol.* 22, No. 1, pp. 2-15, (Jan 1996). Available at: www.dlib.computer.org/ts/books/ts1996/pdf/e0006.pdf [Accessed February 3, 2017]

[4]Bell and LaPadula. (1974). Secure computer systems. ESD-TR-73-278 (Vol. I-III) (also Mitre TR-2547), Mitre Corporation, Bedford, MA, April 1974.

[5]Denning, A. (1976). Lattice model of secure information flow. Comm. ACM Vol. 19, No. 5, pp. 236-243, (May 1976).

[6]Myers and Liskov. (1997). A decentralized model for information flow control, Proc. 16th ACM Symp. Operating Systems Principles, Saint-Malo, pp. 129-142. Available at: www.acm.org/pubs/citations/proceedings/ops/268998/p129-myers
[Accessed February 23, 2017].

[7]Lampson. (1974). Protection, ACM Operating Systems Rev. Vol. 8, No. 1, pp. 18-24, Available at: www.research.microsoft.com/lampson/09-Protection/Abstract.html
[Accessed: February 23, 2017].

[8]Rivest, Shamir, and Adleman. (1978). A method for obtaining digital signatures and public-key cryptosystems. Comm. ACM, Vol. 21, No. 2, pp. 120-126, (Feb., 1978). Available at: www.theory.lcs.mit.edu/~rivest/rsapaper.ps [Accessed February 23, 2016].

[9]Saltzer. (1974). Protection and the control of information sharing in Multics. Communication of the ACM, Vol. 17, No. 7, pp.388-402.

[10]Applegate, S.D. and Stavrou, A. (2013). Towards a Cyber Conflict Taxonomy, 5th International Conference on Cyber Conflict.

[11] Bishop, M. (1995). A Taxonomy of UNIX System and Network Vulnerabilities, University of California at Davis, No. Report CSE-95-10.
Available at: http://citeseerx.ist.psu.edu/viewdoc/summary? Doi=10.1.1.33.5712
[Accessed: February 23, 2017].

[12]Noel, S, Jajodia, S, O'Berry, B., Jacobs, M. (2003). Efficient Minimum-Cost Network Hardening via Exploit Dependency Graphs, in Proceedings of the 19th Annual Computer Security Applications Conference, Las Vegas, Nevada, December, 2003.

[13]Howard, J. D. (1997). An Analysis of Security Incidents on the Internet 1989-1995, Doctoral dissertation, Carnegie Mellon University, Pittsburgh, PA, 1997).
Available at: www.cert.org/archive/pdf/JHThesis.pdf
[Accessed: February 23, 2017].

[14]Killourhy, K. S., Maxion, R. A., & Tan, K. M. C. (2004). A Defense-Centric Taxonomy Based on Attack Manifestation. Presented at the International Conference on Dependable Systems & Networks, Florence, Italy.

[15]Mirkovic, J., & Reiher, P. (2004). A Taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review, 34(2), pp.39-53. Available at: http://dx.doi.org/10.1145/997150.997156 [Accessed: February 23, 2017].

[16]Simmons, C., Ellis, C., Shiva, S., Dasgupta, D., & Wu, Q. (2009). AVOIDIT: A Cyber Attack Taxonomy. Retrieved from http://issrl.cs.memphis.edu/files/papers/ CyberAttackTaxonomy_IEEE_Mag.pdf on 23/2/2016.

[17]Fovino, I. N., Coletta, A., & Masera, M. (2010). Taxonomy of security solutions for the SCADA Sector, Deliverable: D 2.2, Version: 1.1. A European Network For The Security Of Control And Real Time Systems.

[18]Zhu, B., Joseph, A., & Sastry, S. (2011). A Taxonomy of Cyber Attacks on SCADA Systems. IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing. DOI 10.1109/iThings/CPSCom.2011.34.

[19]Gluschke, G., et al. (2015). Cyber Security at Nuclear Facilities: National Approaches: An ISS Research Project in Cooperation with the Nuclear Threat Initiative (NTI).

[20]Dine, A.V., Assante, M., Stoutland, P. (2016). Outpacing Cyber Threats: Priorities for Cyber Security at Nuclear Facilities, The Nuclear Threat Initiative (NTI), CN-244-64.

[21]Nuclear-Security – Measures to protect Against Nuclear Terrorism, Amendment to the Convention on the Physical protection of Nuclear Material (2005) GOV/INF/2005/10-GC(49)/INF/6, IAEA Board of Governors General Conference. Available at: http://www.iaea.org/About/Policy/GC/GC49/Documents/gc49inf-6.pdf
[Accessed: February 23, 2017].

[22]Nuclear Energy Act (1999). Act No. 46 of 1999, NEA. Available at: http://www.energy.gov.za/files/policies/act_nuclear_46_1999.pdf
National Nuclear Regulatory Act (1999) Act No.47 of 1999, NNRA. Available at:
http://www.energy.gov.za/files/policies/act_nuclear_47_1999.pdf
[Accessed: February 23, 2017].

[23] An Act to amend the Atomic Energy Act of 1946, as amended, and for other purposes (1954) The 83rd United States Congress. Available at: http://pbadupws.nrc.gov/docs/ML1327/ML13274A489.pdf# page=23 (pages 7-228). Also known as Atomic Energy Act of 1954 [Accessed: February 23, 2017].
National Nuclear Security Administration Act; 2010

[24] Act on the peaceful utilization of atomic energy and the protection against its hazards (Atomic Energy Act) (1959) Bundestag, AtG. Available at: http://www.gesetze-im-internet.de/bundesrecht/atg/gesamt.pdf [Accessed: February 23, 2017].

[25]There are two Government Decrees that establish fundamental requirements to physical protection (PP) of nuclear materials and nuclear facilities and control and accounting (MC&A) of nuclear materials. These Decrees are:
Regulation on the State System for Nuclear Material Accounting and Control. Enacted by the Government Decree #352 of May 6, 2008.
Rules of the Physical Protection of Nuclear Material, Nuclear Facilities, Nuclear Material Storage Points. Enacted by the Government Decree #456 of July 19, 2007.

[26]Electronic Communications and Transactions Act (2002) Act No. 25 of 2002, ECT. Available at: http://www.itu.int/ITU/projects/ITU_EC_ACP/hipssa/Activities/SA/docs/SA_1_Legislations/South%20Africa/ElecComm.PDF [Accessed: February 23, 2017].
COMSEC Act (2003)
Minimum Information Security Standards (MISS) (1996). Available at: http://www.kzneducation.gov.za/LinkClick.aspx?fileticket=aDNwzVuiANQ%3D&... [Accessed: February 23, 2017].

[27] Protection of secret or OUO information is governed by the: Federal Law "On State Secret" and Federal Law "On Information, Information Technologies and Information Protection." (2006) Duma, No. 149-FZ. Available at: http://old.svobodainfo.org/en/node/441
Draft Law "On Security of Critical Information Infrastructure of Russian Federation" that would cover protection of industrial control systems has been developed by the Federal Security Service (FSB), but has not yet submitted for consideration in Russian legislative body. Above mentioned laws apply to multiple domains, including nuclear security, but nuclear security is not explicitly referenced in these laws.

[28] Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes (2009) Bundestag. Available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/BSI/bsiges2009_pdf.pdf?__blob=publicationFile [Accessed: February 23, 2017].

[29] Pederson, P. (2015). Regulatory Nuclear Cyber Security: The Core Issues. The Langner Group, LLC Whitepaper, U.S.A.

[30] Gluschke, G., Casin, M.H., & Macori, M. (2018): Cyber Security Policies And Critical Infrastructure Protection. Institute for Security and Safety (ISS) Press.

[31] U.S. Department of Homeland Security (DHS) Nuclear Sector Cybersecurity Framework Implementation Guidance for U.S. Nuclear Power Reactors, pp.3-4.

[32] Sylyar, V. (2012): Cyber Security of Safety-Critical Infrastructures: A Case Study for Nuclear Facilities, International Journal of Information and Security, Vol. 28, No. 1, pp. 98-107.