DEVELOPMENT OF A NEW IEC TECHNICAL REPORT ON CYBERSECURITY RISK MANAGEMENT FOR I&C AND ES IN NPP

Michael T Rowland
Sandia National Laboratories
Albuquerque, USA
mtrowla@sandia.gov

John Sladek
Canadian Nuclear Safety Commission
Ottawa, Canada

Edward L. Quinn
Paragon Energy Services
Dana Point, USA

Tighe Smith
Paragon Energy Services
Hurst, USA

Abstract

The International Electrotechnical Commission (IEC) Subcommittee SC45A has been active in development of cybersecurity standards and technical reports on the protection of Instrumentation and Control (I&C) and Electrical Power Systems (ES) that perform significant functions necessary for the safe and secure operation of Nuclear Power Plants (NPP). These international standards and reports advance and promote the implementation of good practices around the world.

The IEC cybersecurity nuclear standards are aligned with documents in the IAEA Nuclear Security Series (NSS) such as NSS 33-T, Computer security of Instrumentation and Control Systems at Nuclear Facilities, and provide additional technical details. These standards also leverage the ISO/IEC 27000 series to ensure that cybersecurity guidance is consistent with practices and approaches found in other sectors. Specifically, IEC 62645, which details key elements of a cybersecurity programme for I&C and ES systems at NPPs, follows ISO/IEC 27001:2013 *Information Security Management Systems*. IEC 63096 details the security controls recommended for I&C and ES at NPPs and follows ISO/IEC 27002, *Code of practice for information security controls.* Both IEC standards have general guidance for risk management but do not refer directly to the detailed guidance provided in ISO/IEC 27005:2018, *Information security risk management.*

This paper provides an overview of the new IEC Technical Report that provides results of a survey of current cyber-risk approaches and practices to cybersecurity risk management for NPPs. The paper will highlight provide the investigated challenges and surveyed cyber-risk approaches, along with TR structure and conclusions.

1. INTRODUCTION

The International Electrotechnical Commission (IEC) is publishing a new Technical Report (TR) IEC 63486:2024 which contains an analysis of cybersecurity risk management methods used for the Instrumentation and Control (I&C) and Electrical Power Systems (ES) systems at NPPs, based upon an international survey. This paper provides a summary or the TR, its development and content.

IEC 62645:2019 (International Electrotechnical Commission, 2019) provides a framework for an NPP cybersecurity programme to protect I&C and ES. The cybersecurity programme is adapted from ISO/IEC 27001:2013 (International Standards Organization, 2013) which identifies the requirements for an information security management system (ISMS). The NPP cybersecurity programme detailed in (International Electrotechnical Commission, 2019), establishes the process for the assignment of security degrees (SD) to I&C and ES. The use of assigned SDs is analogous to the use of information classification in (International Standards Organization, 2013). IEC 62645 (International Electrotechnical Commission, 2019) then provides requirements for cybersecurity of those systems based on the assigned SD. The assignments of SDs to I&C and ES are informed by the safety categorization of the system based which is based upon IEC 61513:2011 (International Electrotechnical Commission, 2011) and IEC 61226:2020 (International Electrotechnical Commission, 2020).

IEC 62645:2019 (International Electrotechnical Commission, 2019), like ISO 27001:2013 (International Standards Organization, 2013), provides a generic framework for risk management. It does not provide detailed

guidance on risk management, other than referring to ISO/IEC 27005:2018 (International Standards Organization, 2018). This provides a potential gap in standardization of specific implementation methods. IEC 62645:2019 (International Electrotechnical Commission, 2019) allows for diversity in risk management methods based upon the organization, its organizational, industrial and regulatory context.

A survey of the national standards for cybersecurity programmes and/or risk management methods was conducted as part of the development of the TR. This TR provides conclusions as to whether there exists enough similarity in these national approaches to progress efforts to standardize these approaches for cybersecurity of NPPs, including Small Modular Reactors. Additionally, the TR will identify variances and diversity of these methods that increases the challenges of operators to apply a common consistent approach to risk management and to benchmark their programmes between countries. The expected publication date of IEC TR 63486 is Q3/4-2024.

2. STANDARDIZATION CONTEXT

The TR follows the top-level documents of the IEC SC45A standard series IEC 61513 (International Electrotechnical Commission, 2011) and IEC 63046 (International Electrotechnical Commission, 2020). IEC 61513 (International Electrotechnical Commission, 2011) provides general requirements for I&C systems and equipment that perform functions important to safety in NPPs. IEC 63046 (International Electrotechnical Commission, 2020) provides general requirements for electrical power systems of NPPs, including the power supplies for the I&C systems. IEC 61513 (International Electrotechnical Commission, 2011) and IEC 63046 (International Electrotechnical Commission, 2020) are to be considered in conjunction and are at the same Standards Level. IEC 61513 (International Electrotechnical Commission, 2011) and IEC 63046 (International Electrotechnical Commission, 2020) define the structure of the IEC SC45A standard series and shape a complete framework establishing general requirements for instrumentation, control and electrical systems for nuclear power plants.

IEC 62645 (International Electrotechnical Commission, 2019) is considered formally as a second level document with respect to IEC 61513 (International Electrotechnical Commission, 2011), although IEC 61513 (International Electrotechnical Commission, 2011) needs to be revised to ensure proper reference to and consistency with IEC 62645 (International Electrotechnical Commission, 2019). IEC 62645 (International Electrotechnical Commission, 2019) is the top-level document with respect to cybersecurity in the SC45A standard series. Other documents are developed under IEC 62645 (International Electrotechnical Commission, 2019) and correspond to third level documents in the IEC SC45A standards.

The placement of the IEC TR within the IEC SC45A standard series for cyber security are illustrated in FIG. 1. below[1]:

[1] IEC Technical Reports focus on a particular subject and contain for example data, measurement techniques, test approaches, case studies, methodologies and other types of information that is useful for standards developers and other audiences. They are never normative. (https://www.iec.ch/publications/technical-reports)

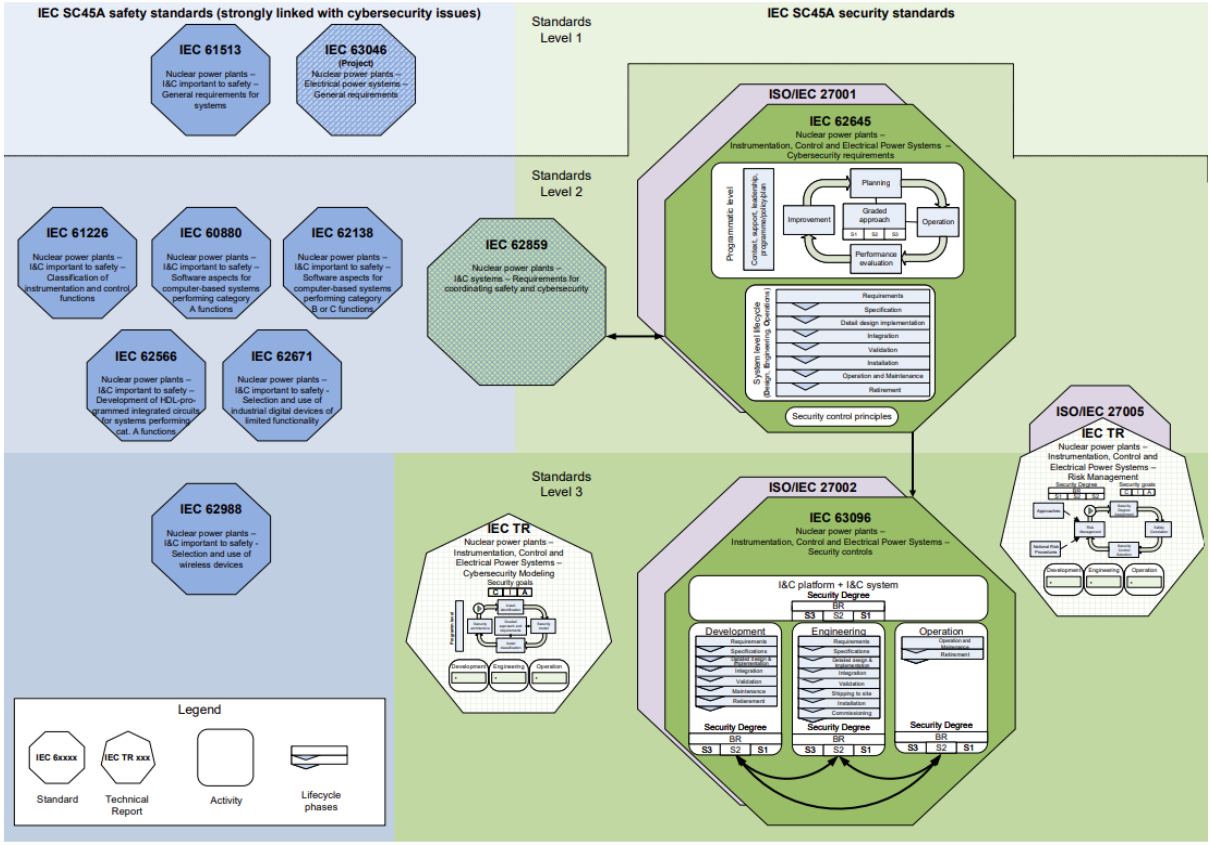

FIG. 1. IEC SC45A NPP Cybersecurity Standards

3. EXISTING GUIDANCE

3.1. IEC 62645 Risk Management Framework

IEC 62645 (International Electrotechnical Commission, 2019) (section 5.4) provides a high-level outline of cyber security management processes adapted from ISO/IEC 27001:2013 (International Standards Organization, 2013). However, IEC 62645 (International Electrotechnical Commission, 2019) does not provide the same level of detailed guidance as ISO/IEC 27005:2018 (International Standards Organization, 2018). This is as a result of IEC 62645 (International Electrotechnical Commission, 2019) scope which "establishes requirements and provides guidance for the development and management of effective computer security programmes for I&C programmable digital systems. Inherent to these requirements and guidance is the criterion that the power plant I&C programmable digital system security programme complies with the applicable country's requirements."

The current approach is to establish a cyber security programme that uses a risk assessment method adapted from ISO 27001 (International Standards Organization, 2013). There is a need for further guidance to aid risk management approaches for NPP cybersecurity programmes similar to the relationship between ISO/IEC 27001 (International Standards Organization, 2013) and ISO/IEC 27005 (International Standards Organization, 2018) to further optimize the allocation of limited resources for cybersecurity at NPPs.

Risk is typically described as the product of consequences and likelihood. However, the application in the nuclear domain tends to prioritize consequence over likelihood. This is a pragmatic assumption as the potentially severe consequences associated with nuclear power plants are unacceptable and cannot occur under any circumstances. Therefore, for instrumentation, control, and electrical systems that are important to safety, a near total reliance on consequence determines the level of effort to ensure these risks are mitigated/reduced to the greatest extent possible.

The IAEA publication (International Atomic Energy Agency, 2021) indicates that defense in depth (DiD) is supported through the specification, establishment, and maintenance of a defensive computer security

architecture (DCSA). The DCSA specification is informed by the applicable computer security model[2] to ensure consistency in defensive posture.

DiD is achieved through the arrangement of computer security zones within a DCSA that provides the greatest protection to those I&C and ES that have the largest security demands (i.e. SD1). The multiple layers within the DCSA aim to provide DiD against unknown or undisclosed vulnerabilities or novel adversary techniques, tactics, and procedures.

3.2. ISO 27005:2018 Risk Management

ISO 27005 [5] provides a generic, domain-independent process for information security risk management. The specific nuclear risks need to be identified are to be based on the applicable Design Basis Threat (DBT) [3]. Additionally, nuclear power is a heavily regulated industry that demands a certain level of effectiveness of cyber-security risk management.

Risk management stages in ISO 27005 [5] that may have importance to SD assignment within the IEC cybersecurity standards are:

1. External Context (e.g. Regulation, Laws, Safety Classification)
2. Internal Context (e.g. Operational Performance, Organization Reputation)
3. Risk Identification (identification of consequences: ISO/IEC 27005 [5] Section 8.2.6) and
4. Risk Analysis (assessment of consequences: ISO/IEC 27005 [5] Section 8.3.2)

4. METHODOLOGY

The TR provides (1) analysis of current guidance in IAEA publications, associated IEC and ISO standards, (2) enumerate and describe the challenges of risk management processes for cybersecurity of nuclear power plants, (3) identify and describe methods that have the potential to reduce or mitigate these challenges and (4) provide a comparative survey of national approaches to allow for inferences to be made in regards to consistency amongst these approaches to consider the development of an international standard on cybersecurity risk management for NPPs.

4.1. Analysis of current guidance

The analysis of current guidance summarized in section 3, focuses on generic cybersecurity risk management processes for ISMS (ISO 27000 series) and elements of IEC 62645 (International Electrotechnical Commission, 2019) and IEC 63096 (International Electrotechnical Commission, 2020). The aim is to provide a cross reference and potential suggestions, clarifications, or enhancements on how to adopt or tailor guidance for NPPs.

The analysis will also extend to the IAEA NSS publications (International Atomic Energy Agency, 2021) (International Atomic Energy Agency, 2018) (International Atomic Energy Agency, 2020) that provide guidance on risk management process, namely the Facility and System Computer Security Risk Management (CSRM) methods. IAEA NSS 17-T (International Atomic Energy Agency, 2021) provides guidance on a process but does not specify the expected outcomes.

4.2. Challenges associated with Risk Management for Cybersecurity of NPPs

The experts of the SC45A subcommittee identified significant challenges with risk management approaches for cybersecurity due to the high consequence events that are either extremely rare or improbable, the

---

[2] Various computer security models have bene proposed that prioritize one or more of the information security properties of Confidentiality, Integrity, or Availability.

[3] IAEA NSS 10-G (International Atomic Energy Agency, 2021) defines DBT as “the attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorized removal or sabotage, against which a physical protection system is designed and evaluated.” Note: physical protection and nuclear security are equivalent in IAEA guidance.

absence of statistically relevant data sets to perform quantitative risk analysis, and lack of well-defined risk acceptance limits for cybersecurity.

The challenges evaluated within the IEC 63486:2024 are listed in Table 1 below:

Table 1 – Risk management challenges

#	Description	Rationale
1	**Aggregate risk of multiple units / locations:** There is a need for additional ways to evaluate levels beyond Security Degree assignment for aggregate risk of multiple units / locations.	The analysis focuses on multiple locations (not co-located), and some clauses of IEC 62645 (International Electrotechnical Commission, 2019) do not address multiple co-located units.
2	**Complexity of interdependencies and interactions:** Identifying and analyzing risks associated with attacks that target more significant functions through their interdependencies and/or interactions with less significant functions.	The NPP may not directly manage risks associated with interdependencies between systems and functions. For example, an attack on a diesel fuel supply may impact standby generator operation or external offsite power.
3	**Incident likelihood determination (leading to extremely rare but unacceptable events):** Estimating the likelihood of an extremely rare but unacceptable event is challenging.	Severe accidents at NPPs are extremely rare and can result in unacceptable radiological consequences. Accidents for which the initiating event is a cyberattack are rare and lack statistical data that would allow for likelihood to be considered in risk analysis and evaluation.
4	**Unknown or lacking sufficient detail for pre-developed components:** Pre-developed components that make up digital I&C systems have not been individually identified and evaluated for risks associated with NPP applications. In these cases, the Operator performs the risk assessment and may incur extra effort to treat risk.	Modern supply chains that result in digital I&C system components are complex. Specifically, the NPP operator is not provided a complete bill of materials and software provenance. This gap in information increases uncertainty in risk management activities.
5	**Differences in cyber-risk management:** Many differing risk management processes are used across or within member states.	The differences between member states' regulations or between organizations within a member state with respect to risk management are significant, especially where the level of abstraction is low (e.g., asset).
6	**Lack of abstract analysis methods:** There exists a general lack of guidance on risk management applied to conceptual facilities, systems, and processes where the technology or operational environment is not completely known. The risk impact has a greater dependence on the controlled process (e.g., primary asset; Domain Based Security) that may be unknown. There is a need to provide additional guidance on performing cybersecurity risk management at an abstract level.	Standard processes that provide for abstract analysis, where functions and levels are considered, are not available for this level of risk assessment. IAEA FCSRM (International Atomic Energy Agency, 2021) and NIST Risk Management Framework (RMF NIST SP800-39 (National Institute of Standards and Technology, U.S. Department of Commerce, 2011) provide for multiple levels of risk management processes based on the level of abstraction to separate the nature and source of risks to simplify tasks and activities associated with risk management.
7	**Uncertainty in vulnerability / susceptibility analysis:** Significant uncertainty is associated with the use of vulnerability / susceptibility analysis / documents necessary for effective risk management.	An unacceptable degree of uncertainty in the quality of vulnerability analysis of an I&C system increases the difficulty in performing effective risk management.
8	**Adversary characterization uncertainty:** Applying a cyber DBT/Adversary analysis to formal risk management of cybersecurity for NPPs is difficult due to the degree of uncertainty associated with adversary analysis in the DBT.	The application of cyber DBT within risk management and the degree of uncertainty associated with adversary analysis (e.g., DBT) increases the difficulty in performing effective risk management.

#	Description	Rationale
9	**Excessive information volume:** Effective and timely analysis of the large volume of information to assess risk is not practical (reasonable).	Modern digital information systems and cybersecurity risk management rely upon a tremendous volume of input data. Rationalizing this amount of information is challenging and could lead to ineffective risk management
10	**Lack of a common and comprehensive risk management process:** There exists a need for a common and comprehensive process that manages all significant risks, both regulatory and organizational objectives.	Significant risks are associated with consequences that will not result in radioactive release or theft of nuclear material (i.e., not required by regulation). The risks that lead to these consequences may not be identified and effectively managed.
11	**Advanced security capabilities incompatibility:** Security controls that provide advanced security capabilities (e.g., Cyber SOC or SIEM, cryptography, virtualization) are unsupported or incompatible with isolated or legacy systems reducing defense in depth and increasing risk.	Contemporary and effective technical measures cannot be implemented on legacy and/or physically isolated systems.

4.3. Cyber-risk Approaches Survey

The TR relied upon the experts of IEC SC45A to provide details of key aspects of cyber-risk management approaches. The survey was completed with responses provided by experts from Canada, France, Germany, Russian Federation, United Kingdom, and United States of America. The variance in the responses was discussed at various IEC Meetings between in October 2020 and May 2024, where it was determined that a template based on ISO 27005 clauses would increase alignment to the specific structure with a list of essential questions.

Once the surveys were completed and compiled, the TR team provided a short summary and conclusion on the level of similarity that may support an update to IEC 62645 (International Electrotechnical Commission, 2019) or the development of a new Risk Management Standard within the IEC SC45A series.

Table 2 – Cyber-risk approaches

Approach	Description	Entity
Facility Computer Security Risk Management (FCSRM) (International Atomic Energy Agency, 2021)	The FCSRM assesses the impacts of compromise on facility functions and strategic risks.	IAEA
System Computer Security Risk Management (SCSRM) (International Atomic Energy Agency, 2021)	The SCSRM assesses the assets, systems, security controls, attack pathways, and tactical risks.	IAEA
EBIOS (Secrétariat général de la défense et de la sécurité nationale Agence nationale de la sécurité des systèmes d'information, 2010) (Secrétariat général de la défense et de la sécurité nationale Agence nationale de la sécurité des systèmes d'information, 2019)	EBIOS provides a formalized approach for assessing and treating risks within the field of information systems security, including support tools for contracting authorities, drafting documents, and raising awareness	Agence nationale de la sécurité des systèmes d'information (ANSSI)[4]
YVLA.12 (STUK, 2021)	YVLA.12 sets out requirements for the management of information security at a nuclear facility, and it specifies in more detail the design requirements outlined in the STUK Regulation on Security in the Use of Nuclear Energy (STUK 3/2020)	Finland
IEC 62443 (International Electrotechnical Commission, 2009)	IEC 62443 provides a series of standards with a focus on Operational Technology (OT). The IEC 62443 considers systems and components in risk informing requirements and implementation of security controls.	IEC

Approach	Description	Entity
Cyber Informed Engineering (CIE) (Anderson, Benjamin, Wright, Quinones, & Paz, 2017)	CIE provides a framework for understanding and addressing cyber threats to NPP systems and facilities.	US Department of Energy (DOE)
Hazards and Consequences Analysis for Digital Systems (HAZCADS (Energy Power Research Institute, 2018))	HAZCADS leverages Systems Theoretic Process Analysis (STPA) to identify Unsafe Control Actions (UCAs) within control systems that may result from faults including those caused by cyberattacks. This analysis allows for risk-informed hazard analysis and selection of security controls.	Electric Power Research Institute (EPRI)
Harmonized Threat Risk Assessment (HTRA) (Government of Canada, Communications Security Establishment/Royal Canadian Mounted Police, 2007)	HTRA provides a scalable framework to address strategic and tactical risks. HTRA provides several tools and tables to simplify the risk management processes.	Canada
Malicious Acts Guidelines for Computer-Based Systems (SEWD) (Weisbaum, 2020)	These guidelines are “classified information – for official use only” and not publicly available. They cover the whole IT-security framework for the nuclear field with some parts for cyber risks.	Germany
Information Security Technology—Implementation Guide to Risk Assessment of Industrial Control Systems GB/T 36466 (GB Standards, 2018)	The national standard GB/T 36466-2018 “Information security technology—Implementation guide to risk assessment of industrial control systems” provides guidelines for cyber security assessment for industrial control systems.	China
Regulatory Guide (RG) 5.71 (United States Nuclear Regulatory Commission, 2010)	RG 5.71 provides one acceptable approach regarding the protection of digital computers, communications systems, and networks from a cyber- attack as defined by Title 10 Code of Federal Regulations (CFR) Part 73.1 (United States Nuclear Regulatory Commission, 2017)	US Nuclear Regulatory Commission (NRC)
Information Assurance Standard 1/2; Domain Based Security (IS/DBSy) (United Kingdom Cabinet Office - National Technical Authority for Information Assurance, 2009) (United Kingdom Cabinet Office - National Technical Authority for Information Assurance, 2008)	The standard consists of two parts. The first part provides a detailed Technical Risk Assessment methodology delivered through 6 steps and supported by the Domain Based Security (DBSy) asset modelling technique. The second part includes a 4-step methodology for Risk Treatment that is based on the selection of controls from ISO/IEC 27002 . The methodology will be referred further in this report as UK IS/DBSy.	United Kingdom
Protection of critical infrastructure, including I&C Systems (Russian Federation, 2017) (Russian Federation, 2017)	A set of laws at the state level which regulate the basic norms of the protection of critical infrastructure, including I&C Systems. Standards issued by Federal Service for Technical and Export Control (FSTEC) covering the security risk assessment	Russian Federation

5. IEC TR 63486 CYBERSECURITY RISK MANAGEMENT

This scope of TR is to capture the national and international approaches employed to manage cyber-security risks associated with I&C and Electrical Systems at a Nuclear Power Plant (NPP). This report will relate the various international and national approaches used at NPPs with the Risk Management Stages identified in ISO/IEC 27005:2018 (International Standards Organization, 2018).

5.1. Structure

The structure of IEC TR 63486 is as follows:

- Introduction
- Scope
- Normative References
- Terms and Definitions
- Abbreviated Terms
- IEC 62645 Risk Management Elements
- NPP Cyber Risk Management Challenges and Analyses
- Cyber Risk Approaches vs. Challenges by ISO/IEC 27005 Clause
- Conclusions
- Annexes detailing the analysis of Cyber risk approaches

6. CONCLUSION

IEC TR 63486 details the similarities and differences in cyber security risk management processes at nuclear power plants throughout the world. Surveyed cyber-risk approaches share many common elements with ISO/IEC 27005:2018 [5] while addressing some or all identified challenges. Additionally, the guidance within these cyber-risk approaches enhances (builds upon) the existing framework of IEC 62645 [1] with respect to risk management. The cyber-risk approaches are complementary and not contradictory, as detailed in the analysis of Annexes.

The strong association of the IEC SC45A cybersecurity standards with the ISO 27000 series of standards lends itself to support for an IEC SC45A standard aligned with ISO 27005:2018 (International Standards Organization, 2018). The importance of the cyber risk approaches survey is critical in the determination on the level of similarity that would support an update to IEC 62645 (International Electrotechnical Commission, 2019) or development of a new Risk Management Standard. A future IEC risk management standard for NPP operators may consider the identified key insights from the cyber-risk approaches evaluated for this technical report.

ACKNOWLEDGEMENTS

Sandia National Laboratories is a multi-mission 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.

This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

The authors also acknowledge the contributions of Thomas Walter (Figure 1), and the IEC TR development team (Steve Batson, Juergen Bochtler, Nicolas Chevaux, Jan Degreick, Ismael Garcia, Yun Guo, Leroy Hardin, Jianghai Li, Paul Lajoie-Mazanc, Kim Lawson-Jenkins, Jennifer Marek, Kimberly Mitchell, Ludovic Pietre-Cambacedes, Vitaly Promyslov, Robert Valkama, Guido Villacis-Rivas, Karl Waedt, Fan Zhang)

REFERENCES

Government of Canada, Communications Security Establishment/Royal Canadian Mounted Police. (2007). *Harmonized Threat and Risk Assessment Methodology.* Ottawa: CSE.

Anderson, R., Benjamin, J., Wright, V., Quinones, L., & Paz, J. (2017). *INL/EXT-16-40099 Rev 0: Cyber-Informed Engineering.* Idaho Falls: INL.

Energy Power Research Institute. (2018). *EPRI TR 3002012755 HAZCADS – Hazards and Consequences Analysis for Digital Systems, .* Palo Alto: EPRI.

GB Standards. (2018). *GB?T 36466-2018: Information Security Technology - Implementation guide to risk assessment of industrial contorl systems.* Beijing: GB Standards.

International Atomic Energy Agency. (2018). *IAEA Nuclear Security Series No. 33-T Computer Security of Instrumentation and Control Systems at Nuclear Facilities, Technical Guidance Reference Manual.* Vienna: IAEA.

International Atomic Energy Agency. (2020). *IAEA Nuclear Energy Series No. NR-T-3.30 Computer Security Aspects of Design for Instrumentation and Control Systems at Nuclear Power Plants.* Vienna: IAEA .

International Atomic Energy Agency. (2021). *Implementing Guide: National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements, NSS 10-G Rev 1.* Vienna: IAEA.

International Atomic Energy Agency. (2021). *Technical Guidance, Computer Security Techniques at Nuclear Facilities, NSS 17-T.* Vienna: IAEA.

International Electrotechnical Commission. (2009). *IEC TS 62443-1-1:2009, Industrial communication network - Network and system security - Part 1.1: Terminology, concepts and models.* Geneva: IEC.

International Electrotechnical Commission. (2011). *IEC 61513:2011 Nuclear power plants - Instrumentation and control important to safety - General requirements for systems.* Geneva: IEC.

International Electrotechnical Commission. (2019). *IEC 62645:2019 - Nuclear Power Plants - Instrumentation, control, and electrical power systems - Cybersecurity requirements.* Geneva: IEC.

International Electrotechnical Commission. (2020). *IEC 61226:2020 Nuclear power plants - Instrumentation, control and electrical power systems important to safety - Categorization of functions and classification of systems.* Geneva: IEC.

International Electrotechnical Commission. (2020). *IEC 63046:2020 - Nuclear Power Plants - Electrical power system - General requirements.* Geneva: IEC.

International Electrotechnical Commission. (2020). *IEC 63096:2020 - Nuclear power plants - Instrumentation, control and electrical power systems - Security controls.* Geneva: IEC.

International Standards Organization. (2013). *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements.* Geneva: ISO/IEC.

International Standards Organization. (2018). *ISO/IEC 27005:2018 — Information technology — Security techniques — Information security risk management.* Geneva: ISO.

National Institute of Standards and Technology, U.S. Department of Commerce. (2011). *NIST Special Publication 800-39 - Managing Information Security Risk: Organization, Mission, and Information System View.* Gaithersburg: NIST.

Russian Federation. (2017). *Federal Law of July 26, 2017 N 187-FZ On the security of critical information infrastructure of the Russian Federation (in Russian).* Moscow: Russian Federation.

Russian Federation. (2017, 07 27). *Federal Law of July 27, 2006 No. 149-FZ (as amended on December 19, 2016) "On Information, Information Technologies and the Protection of Information". (in Russian).* Retrieved 08 16, 2020, from https://legalacts.ru/doc/FZ-ob-informacii-informacionnyh-tehnologijah-i-o-zawite-informacii/

Secrétariat général de la défense et de la sécurité nationale Agence nationale de la sécurité des systèmes d'information. (2010). *Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) - Méthode de Gestion des Risques.* Paris: ANSSI.

Secrétariat général de la défense et de la sécurité nationale Agence nationale de la sécurité des systèmes d'information. (2019). *EBIOS Risk Manager / An Iterative Approach in 5 Workshops.* Paris: ANSS.

STUK. (2021). *Information security management of a nuclear facility, 12.2.2021.* Retrieved 04 25, 2022, from https://www.stuklex.fi/en/ohje/YVLA-12

United Kingdom Cabinet Office - National Technical Authority for Information Assurance. (2008). *HMG IA Standard No. 2: Risk Management & Accreditation of Information Systems, 2008-10, Issue No. 3.1.* Cheltenham: CESG.

United Kingdom Cabinet Office - National Technical Authority for Information Assurance. (2009). *HMG IA Standard No. 1 Technical Risk Assessment .* Cheltenham: CESG.

United States Nuclear Regulatory Commission. (2010). *Regulatory Guide 5.71 - Cyber Security Programs for Nuclear Facilities.* Rockville: NRC.

United States Nuclear Regulatory Commission. (2017, 08 29). *10 Code of Federal Regulations § 73.1 Purpose and scope.* Retrieved 08 16, 2020, from https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0001.html

Weisbaum, A. (2020). Address IT-Security in nuclear security regulation and implementation (CN-278-248). *Proceedings on International Conference on Nuclear Security (ICoNS).* Vienna: IAEA.