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.

SAND2021-4630C

Development of a new IEC Technical Report on Cybersecurity Risk Management for I&C and ES in Nuclear Power Plants

Michael T Rowland
Sandia National Laboratories
PO Box 5800, 0748 Albuquerque, NM 87185 USA
mtrowla@sandia.gov

Edward L. Quinn
Technology Resources
23292 Pompeii Drive Dana Point, CA 92629, USA
tedquinn@cox.net

John Sladek
Canadian Nuclear Safety Commission
280 Slater St., Ottawa, ON, Canada, K1P 4S9
John.Sladek@canada.ca

[Digital Object Identifier (DOI) placeholder]

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 development of a new IEC Technical Report (TR) that surveys current approaches to and practices for cybersecurity risk management for NPPs. The TR will highlight similarities and differences in national approaches, advances in risk management practices, summarize updates to risk guidance in IAEA publications, and recommend potential activities that aim to standardize good risk management practices for cybersecurity at NPPs.

Key Words: IEC, cybersecurity, risk management, standards

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.

1 INTRODUCTION

The International Technical Commission (IEC) is developing a new Technical Report (TR) 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 an overview of the development, content and status of the draft TR.

IEC 62645:2019 [1] provides a framework for an NPP cybersecurity programme to protect I&C and ES. The cybersecurity programme is adapted from ISO/IEC 27001:2013 [2] which identifies the requirements for an information security management system (ISMS). The NPP cybersecurity programme detailed in [1], 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 [2]. IEC 62645 [1] 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 [3] and IEC 61226:2020 [4].

IEC 62645:2019 [1], like ISO 27001:2013 [2], provides a generic framework for risk management. It does not provide detailed guidance on risk management, other than referring to ISO/IEC 27005:2018 [5]. This provides a potential gap in standardization of specific implementation methods. IEC 62645:2019 [1] allows for diversity in risk management methods based upon the organization, and 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 intends to provide conclusions as to whether there is enough similarity in these national approaches to progress efforts to standardize these approaches for cybersecurity of NPPs. The TR will also identify variances and diversity in these methods which increase the challenges to operators in applying a common consistent approach to risk management and in benchmarking their programmes against programmes from other countries.

2 STANDARDIZATION CONTEXT

The TR follows the top-level documents of the IEC SC45A standard series IEC 61513 [3] and IEC 63046 [6]. IEC 61513 [3] provides general requirements for I&C systems and equipment that perform functions important to safety in NPPs. IEC 63046 [6] provides general requirements for electrical power systems of NPPs, including the power supplies for the I&C systems. IEC 61513 [3] and IEC 63046 [6] are to be considered in conjunction and are at the same Standards Level. IEC 61513 [3] and IEC 63046 [6] 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 [1] is considered formally as a second level document with respect to IEC 61513 [3], although IEC 61513 [3] needs to be revised to ensure proper reference to and consistency with IEC 62645 [1]. IEC 62645 [1] is the top-level document with respect to cybersecurity in the SC 45A standard series. Other documents are developed under IEC 62645 [1] and correspond to third level documents in the IEC SC 45A standards.

The placement of the IEC TR within the IEC SC45A standard series for cyber security are illustrated in Figure-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)

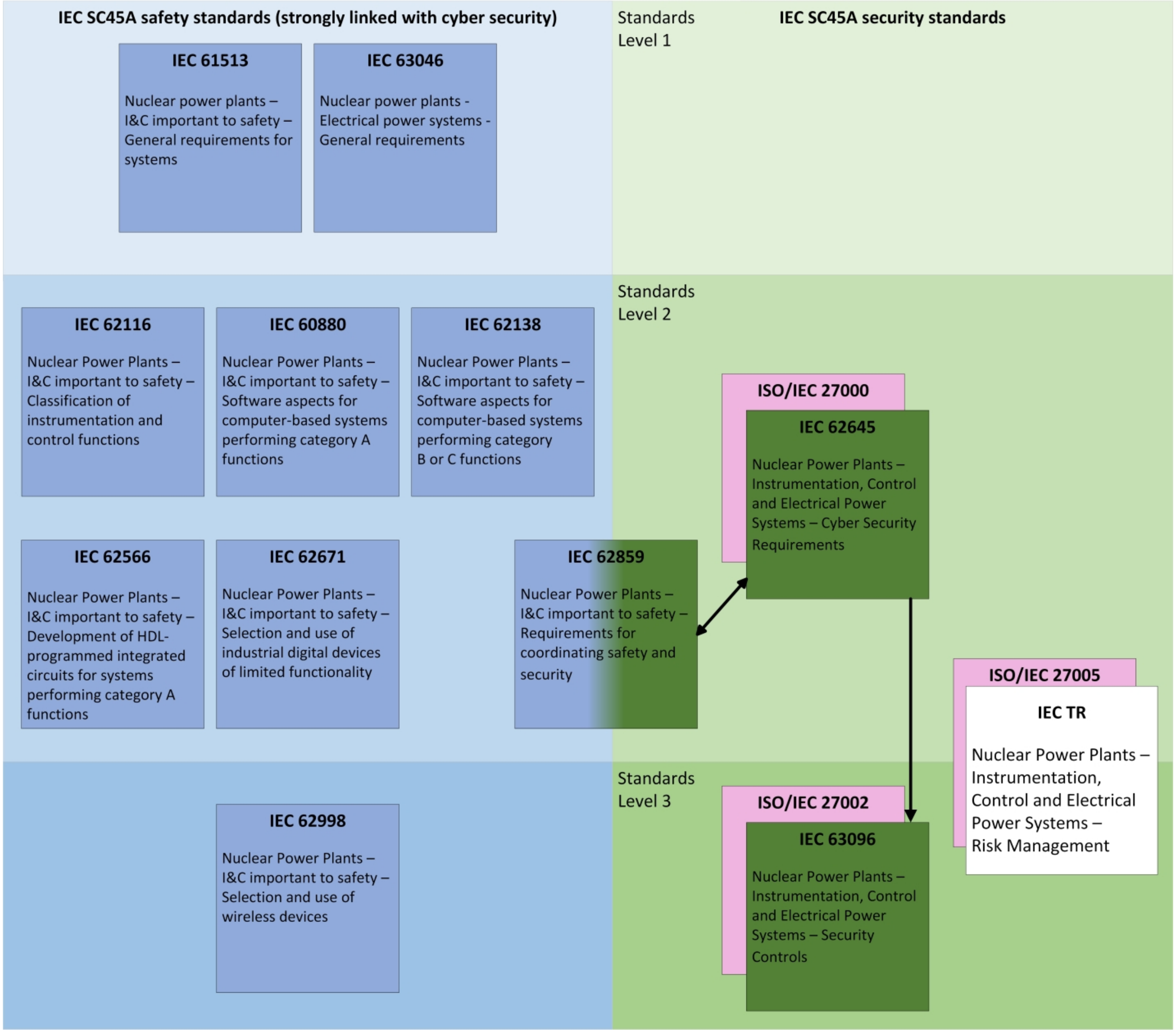
IEC SC45A safety standards (strongly linked with cyber security)
Standards Level 1
IEC SC45A security standards
IEC 61513
Nuclear power plants – I&C important to safety – General requirements for systems
IEC 63046
Nuclear power plants - Electrical power systems - General requirements
Standards Level 2
IEC 62116
Nuclear Power Plants – I&C important to safety – Classification of instrumentation and control functions
IEC 60880
Nuclear Power Plants – I&C important to safety – Software aspects for computer-based systems performing category A functions
IEC 62138
Nuclear Power Plants – I&C important to safety – Software aspects for computer-based systems performing category B or C functions
ISO/IEC 27000
IEC 62645
Nuclear Power Plants – Instrumentation, Control and Electrical Power Systems – Cyber Security Requirements
IEC 62566
Nuclear Power Plants – I&C important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions
IEC 62671
Nuclear Power Plants – I&C important to safety – Selection and use of industrial digital devices of limited functionality
IEC 62859
Nuclear Power Plants – I&C important to safety – Requirements for coordinating safety and security
ISO/IEC 27005
IEC TR
Nuclear Power Plants – Instrumentation, Control and Electrical Power Systems – Risk Management
Standards Level 3
IEC 62998
Nuclear Power Plants – I&C important to safety – Selection and use of wireless devices
ISO/IEC 27002
IEC 63096
Nuclear Power Plants – Instrumentation, Control and Electrical Power Systems – Security Controls

Figure 1. IEC SC45A Standards associated with Cybersecurity (adapted from IEC 63096 [10])

3 EXISTING GUIDANCE

3.1 IEC 62645 Risk Management Framework

IEC 62645 [3] (section 5.4) provides a high-level outline of cyber security management processes adapted from ISO/IEC 27001:2013 [2], but does not provide the same level of detailed guidance as ISO/IEC 27005:2018 [2]. This is because of IEC 62645's [3] 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 [2]. There is a need for further guidance regarding risk management approaches for NPP cybersecurity programmes, similar to the relationship between ISO/IEC 27001 [2] and ISO/IEC 27005 [5], to optimize further the allocation of limited resources for cybersecurity at NPPs.

Risk is typically described as the product of consequences and likelihood, but 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.

3.1.1 Assignment of Security Degrees

IEC 62645 [3] (Section 5.4.3.1.1.2) outlines a classification scheme that is based upon the following principles (1) consequences of cyberattack affecting safety are considered to be more serious than consequences affecting plant performance; (2) assessment of systems is based upon the functions that they implement, and the SD assigned to a system is based upon the function which leads to the most severe impact when compromised; and (3) the resulting consequence-based method for assigning I&C and ES to a particular SD is rigorous and repeatable.

The application of a graded approach is intrinsically linked to consequences in the NPP and subsequently directly linked to SDs. There are three SDs that range from SD1, which has the most demanding cybersecurity requirements (i.e., I&C or ES associated with the greatest consequences), to SD3, which has the least demanding cybersecurity requirements (i.e., I&C or ES associated with the lesser consequences). Baseline requirements apply to all I&C and ES regardless of their SD assignment.

Each SD consists of baseline requirements and a unique set of requirements that when imposed upon I&C and ES provide the level of protection that is appropriate and necessary. It is possible that one or more requirements for a particular SD are the same as for other SDs; however, the complete set of requirements is unique for each security degree (i.e., SD1, SD2, SD3).

3.1.2 Security Zones

IEC 62645 [3] (section 5.4.3.3) outlines the concept of security zones, which allows for grouping together I&C and ES assets to simplify the administration and application of protective measures. IAEA NSS 33-T [7], NST047 [8] and IAEA NES No. NR-T-3.30 [9] provide additional guidance on computer security zones. Paragraph 2.28 of [7] states, "The security zone concept involves the logical and/or physical grouping of computer-based systems that share common security requirements, due to inherent properties of the systems or their connections to other systems. All systems located within a single zone are protected at the same security level, namely that assigned to the I&C system function with the most stringent security level within the zone."[2]

The definition of zones shall comply with the security degree, I&C and security architecture requirements. The IAEA publications [7] [8] [9] specifically indicate that the security architecture[3] requirements are necessary to ensure computer security Defense in Depth (DiD).

Security Zones are necessary to ensure consistency in implementing computer security.

3.1.3 Defense in Depth

IEC 62645 [3] Section 7.3 states "Security defence-in-depth is an approach to security in which multiple and independent security controls, covering organizational, technical and operational aspects, are deployed in an architecture, as no individual security control can provide the expected security. In such approach, it

[2] IAEA publications use the term "Security Level" which is broadly equivalent to the IEC term of "Security Degree". This paper will use the term Security Degree to represent both.

[3] IAEA Publications refer to the security architecture as the Defensive Computer Security Architecture (DCSA)

is the set of diversified and independent security controls which is able to bring the needed prevention, detection and response capabilities."

The IAEA publication [8] indicates that 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[4] 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.

3.1.4 IEC 63096:2020 Controls Catalogue

IEC 62645 [1] and the IAEA publications [7] [8] use a consequence-informed approach in the assignment of SDs. The SDs are associated with a set of requirements and a set of recommend controls listed in IEC 63096 [10]. IEC 63096 [10] sorts these controls into three distinct phases, Platform Development (D), Project Engineering (E) and Operations and Maintenance (O). IEC 63096 provides a mapping of the DEO phases to the IAEA NSS 33-T [7] and SSG-39 [11] system lifecycle which allows for simple referencing of the IEC control to the requirement or to IAEA guidance.

The DEO phases were necessary to inform vendor-operator risk management arrangements and to simplify acceptance of pre-developed items and/or platforms for I&C or ES assigned to a SD. For example, if a platform or system were developed and qualified to a specific SD, it would reduce the operator's effort in verifying compliance to an NPP cybersecurity programme based upon IEC 62645 [1].

3.2 ISO 27000 Series

The ISO 27000 series standards provide guidance on aspects of ISMSs. Specifically, the standards of importance to the IEC NPP cybersecurity standards are:

- ISO 27001 [2] associated with IEC 62645 [1]
- ISO 27002 [12] associated with IEC 63096 [10]
- ISO 27005 [5] important to the IEC TR.

3.3 ISO 27001:2013 Risk Management Framework

The framework within 27001 [2] is strongly aligned with ISO 31000:2018 [13]. Risk is defined within ISO 31000 as "effect of uncertainty on objectives". ISO 27001 [2] risk framework consists of major parts (Clauses 6.1.2 – risk assessment and 6.1.3 – risk treatment). There are three main components of risk assessment: (1) risk identification, (2) risk analysis (e.g., determine level of risk), and (3) risk evaluation (e.g., prioritize analyzed risks for treatment).

IEC 62645 [1] (section 5.4.3) contains the adapted guidance for the associated sections of ISO 27001 [2]. The effect of these adaptations is to significantly rely on consequence when determining the level of risk (impacting risk analysis) and assigning SDs as a means of prioritizing analyzed risks for treatment (impacting risk evaluation).

ISO 27001 [2] provides a normative annex, Annex A, which lists reference control objectives and controls that are to be used in context with Clause 6.1.3 (risk treatment). Annex A is aligned and derived from ISO 27002 [12] and forms the basis for the production of the Statement of Applicability required by Clause 6.1.3 (d).

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

3.3.1 ISO 27002:2013 Information Security Controls

ISO 27002 is a valuable controls catalogue that provides additional detail on how to implement the reference control objectives and controls listed in Annex A. The use of this standard increases consistency in approaches and quality in implementing controls necessary for a continually improving ISMS. ISO 27002 [12] formed the basis of IEC 63096 and the ISO guidance was adapted where necessary to be feasible for NPP cybersecurity programmes developed under IEC 62645 [1].

3.3.2 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)[5]. 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 will (1) provide an 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. The TR is intended to be used by SC45A when considering the development of an international standard on cybersecurity risk management for NPPs.

4.1.1 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 [1] and 63096 [10]. 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 [8] [9] [10] that provide guidance on risk management process, namely the Facility and System Computer Security Risk Management (CSRM)methods. Also, IAEA NST047 [9] provides guidance on a process but does not specify the expected outcomes.

4.1.2 Current Challenges

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

[5] IAEA NSS 10-G (To be published) 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.

These challenges involving likelihood and probability (e.g., high consequence events involving complicated scenarios that have yet to be demonstrated) combined with the lack of operating experience (e.g., no relevant datasets) will be investigated and described in the TR. A key objective of the TR is to provide insights for risk management processes that can improve outcomes and increase consistency.

4.1.3 Methods supportive of Risk Management Elements

The TR will also detail advances in Risk Management methods that may support cybersecurity risk management. These frameworks include (1) IAEA Facility and System CSRMs [8] [9] [10], (2) France EBIOS [14], (4) Consequence Reduction, (5) Hazards and Consequences Analysis for Digital Systems (HAZCADS) [14], (6) Cyber Informed Engineering [14], (7) Pathway/Susceptibility Analysis [16], (8) Scenario analysis based on IEC 62645 [1] and 63096 [10] guidance, and (9) Domain Based Security (DBSy) [18] [19]. The objective in detailing these advances is to promote discussion as to the benefits, costs, and limits of these methods.

4.1.4 National Approaches Survey

The TR relies upon the experts of IEC SC45A to provide details of key aspects of their national risk management approach. The initial survey completed with responses provided by experts from Canada [15], France [16], Germany [17], Russian Federation [18], United Kingdom [24, 25], and United States of America [26] [27]. The variance in the responses was discussed at the IEC General Meeting in October 2020, where it was determined that a template would be developed to mandate a specific structure and provide a list of essential questions. The proposed questions are currently under development.

Once the surveys are completed and compiled, the TR team will perform an analysis to determine the level of similarity that may support an update to IEC 62645 [1] or the development of a new Risk Management Standard within the IEC SC45A series.

5 IEC TR 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 [5].

The proposed structure of the TR is as follows:

- Scope
- Limitations
- Normative References
- Terms and Definitions
- Abbreviated Terms
- IEC NPP Cybersecurity Risk Management
- ISO 27005 Adjustments
- Member States Survey of Current Practice

- Advances in Risk Management Methods
- Annexes on Primary and Support Assets Based Graded Risk Management, IEC 62443, and Supply Chain Risk Management,

6 CONCLUSION

The current draft of the TR details the similarities and differences in cyber security risk management processes at nuclear power plants throughout the world. 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 [5]. However, the TR team has not yet completed the analysis necessary to gain insight into the value of undertaking an effort to provide nuclear-specific enhancements or customizations in a potential new International Standards.

IAEA NST047 [9], although approved for publication, has yet to be published. This has impacted the potential for widespread adoption of and gaining experience in the risk management processes detailed within.

The TR team has identified that it may be useful to identify the common techniques that can be applied to all stages, and those other important techniques that may be applied to one or more lifecycle stages. This would go beyond the current scope of the draft TR, but may be included as part of an annex.

Risk acceptance criteria is very challenging especially for nuclear. There is general uncertainty in the level of risk that is acceptable (especially for the lower/less stringent security degrees). Risk is generally described in terms of likelihood and consequence. Due to the deep uncertainty associated with likelihood of cyber-attack resulting in unacceptable radiological consequences, a conservative approach is taken whereby risk is consequence-informed (i.e., dominated).

The importance of the national risk approaches survey is critical in the determination on the level of similarity that would support an update to IEC 62645 [1] or development of a new Risk Management Standard. The expected completion date of the first committee draft is Q3-2021.

7 ACKNOWLEDGMENTS

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, the United States Government. or the Government of Canada.

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, Leroy Hardin, Jianghai Li, Kimberly Mitchell, Ludovic Pietre-Cambacedes, Vitaly Promyslov, Karl Waedt, Fan Zhang)

8 REFERENCES

[1] International Electrotechnical Commission, "IEC 62645:2019 - Nuclear Power Plants - Instrumentation, control, and electrical power systems - Cybersecurity requirements," IEC, Geneva, 2019.

[2] International Standards Organization, "ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements," ISO/IEC, Geneva, 2013.

[3] International Electrotechnical Commission, "IEC 61513:2011 Nuclear power plants - Instrumentation and control important to safety - General requirements for systems," IEC, Geneva, 2011.

[4] International Electrotechnical Commission, "IEC 61226:2020 Nuclear power plants - Instrumentation, control and electrical power systems important to safety - Categorization of functions and classification of systems," IEC, Geneva, 2020.

[5] International Standards Organization, "ISO/IEC 27005:2018 — Information technology — Security techniques — Information security risk management," ISO, Geneva, 2018.

[6] International Electrotechnical Commission, "IEC 63046:2020 - Nuclear Power Plants - Electrical power system - General requirements," IEC, Geneva, 2020.

[7] International Atomic Energy Agency, "IAEA Nuclear Security Series No. 33-T Computer Security of Instrumentation and Control Systems at Nuclear Facilities, Technical Guidance Reference Manual," IAEA, Vienna, 2018.

[8] International Atomic Energy Agency, "NST047 - Computer Security Techniques at Nuclear Facilities," IAEA, Vienna, TBD.

[9] International Atomic Energy Agency, "IAEA Nuclear Energy Series No. NR-T-3.30 Computer Security Aspects of Design for Instrumentation and Control Systems at Nuclear Power Plants," IAEA , Vienna, 2020.

[10] International Electrotechnical Commission, "IEC 63096:2020 - Nuclear power plants - Instrumentation, control and electrical power systems - Security controls," IEC, Geneva, 2020.

[11] International Atomic Energy Agency, "IAEA Safety Standards Specific Safety Guide No. SSG-39 Design of Instrumentation and Control Systems for Nuclear Power Plants," IAEA, Vienna, 2016.

[12] International Standards Organization, "ISO/IEC 27002:2013 - Information technology — Security techniques — Code of practice for information security controls," ISO, Geneva, 2013.

[13] International Standards Organization, "ISO 31000:2018 - Risk management — Guidelines," ISO, Geneva, 2018.

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

[15] Energy Power Research Institute, "EPRI TR 3002012755 HAZCADS – Hazards and Consequences Analysis for Digital Systems,," EPRI, Palo Alto, 2018.

[16] R. Anderson, J. Benjamin, V. Wright, L. Quinones and J. Paz, "INL/EXT-16-40099 Rev 0: Cyber-Informed Engineering," INL, Idaho Falls, 2017.

[17] United States Nuclear Regulatory Commission, "NUREG/CR-6827- Cyber Securtiy Self-Assessment Method for U.S. Nuclear Power Plants," U.S. NRC, Washington, D.C., 2004.

[18] United Kingdom Cabinet Office - National Technical Authority for Information Assurance, "HMG IA Standard No. 1 Technical Risk Assessment," CESG, Cheltenham, 2009.

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

[20] Canadian Standards Association Group, "CSA N290.7-20 - N290.7-14 - Cyber Security For Nuclear Facilities," CSA Group, Toronto, 2020.

[21] République française, Légifrance, "Arrêté du 10 mars 2017 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Nucléaire » et pris en application," Légifrance, 17 03 2017. [Online]. Available: https://www.legifrance.gouv.fr/eli/arrete/2017/3/10/PRMD1703203A/jo/texte. [Accessed 16 08 2020].

[22] Bundesamt für Sicherheit in der Informationstechnik, "BSI Standard 200-3 Risk Analysis based on IT-Grundshutz Version 1.0," BSI, Berlin, 2017.

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

[24] U.K. Office of Nuclear Regulation, "Risk informed regulatory decision making," ONR, London, 2017.

[25] United Kingdom Office for Nuclear Regulation, "ONR Guide: Effective Cyber and Information Risk Management; CNS-TAST-GD-7.1 Revision 1," ONR, Bootle, 2020.

[26] Nuclear Energy Institute, "NEI 08-09 Revision 6, Cyber Security Plan for Nuclear Power Reactors," NEI, Washington, D.C., 2010.

[27] United States Nuclear Regulatory Commission, "Regulatory Guide 5.71 - Cyber Security Programs for Nuclear Facilities," NRC, Rockville, 2010.