DOI: 10.2507/37th.daaam.proceedings.xxx

A CONSOLIDATED AND STANDARDIZED MODEL FOR IT/OT CYBERSECURITY IMPLEMENTATION IN SMALL MODULAR REACTORS (SMRS)

Ales Navratil & Vojtech Kresalek, PhD

Working Paper of 37th DAAAM Symposium

This Publication has to be referred as: Navratil, A[les] & Kresalek, V[ojtech] (2026). A Consolidated and Standardized Model for IT/OT Cybersecurity Implementation in Small Modular Reactors (SMRs) of the 37th DAAAM International Symposium, pp.xxxx-xxxx, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-xx-x, ISSN 1726-9679, Vienna, Austria
DOI: 10.2507/37th.daaam.proceedings.xxx

Abstract

The development of Small Modular Reactors (SMRs) constitutes a significant technological advancement in the nuclear energy sector. These systems are expected to feature modular architecture, reduced installed capacity, and a high-level digitalization of operational processes. The ongoing digital transformation of modern nuclear technologies will enable advanced monitoring, automation, and operational control. A key characteristic of these systems is the integration of Information Technology (IT) and Operational Technology (OT) infrastructures. In the context of nuclear facilities, such integration must be designed and implemented to prevent security breaches and ensure the continued safety, reliability, and resilience of critical systems. This paper addresses the identified research gap by proposing a consolidated IT/OT security implementation model for SMR environments. The proposed model integrates the requirements of nuclear safety, cybersecurity, information security, and operational resilience into a unified framework that supports security risk management throughout the entire SMR life cycle. The model is based on the integration of the requirements specified in IEC 61226, IEC 60880, IEC 62138, IEC 61513, IEC 62443, IEC 62645, the ISO/IEC 27000 series, and the NIS2 Directive. It establishes a reference framework for the design, implementation, and operation of digitally controlled next-generation nuclear facilities.

Keywords: Small Modular Reactors; Information Technology; Operational Technology; Artificial Intelligence; Digital Twins.

1. Introduction

Digitalization is one of the key trends in the modern energy sector [1]. In the case of SMRs, the implementation of digital control systems significantly improves operational efficiency, safety, and reliability [2], [3]. Modern instrumentation and control (I&C) systems utilize extensive networks of sensors, control units, and analytical tools that enable continuous monitoring of operational parameters. The resulting data are leveraged for predictive maintenance, operational optimization, and to support operators' decision-making [2], [4]. In the SMR environment, digitalization is even more significant, as the modular architecture of the reactors allows for the standardization of digital control systems

and their integration into centralized monitoring platforms [1], [2]. However, as the level of digitalization increases, the underlying technological infrastructure becomes inherently more complex, thereby giving rise to security vulnerabilities. These primarily involve cyber threats. Consequently, establishing a unified and comprehensive security concept across all SMR systems is crucial [5], [6].

2. The Impact of Digitalization on Security

The digitization of industrial systems brings several benefits, yet at the same time leads to an increase in the complexity of the cybersecurity environment [7], [8]. One of the main challenges is the dynamic nature of cyber threats and the difficulty of detecting cyberattack vectors [7]. The integration of digital systems creates new communication channels that could potentially be exploited by attackers [8]. Another complication is the complexity of managing security measures. Modern energy systems include numerous devices and software components that must be properly configured and regularly updated [9]. For this reason, it is essential to harmonize or, where appropriate, amend the legislative and regulatory framework. Furthermore, there must be clarity in the concept of cybersecurity, based on a multi-layered approach that integrates strategic security management, process management, and technological measures [9], [10]. In the context of SMRs, it remains necessary to adhere to principles that mandate the independence of safety systems from external networks. Moreover, the reactor systems themselves must be controlled locally and in isolation. Only support functions may utilize cloud technologies. Consequently, SMR systems must continue to function even in the event of a complete loss of internet connectivity or a total failure of external communications [11], [12], [13]. Figure 1 shows the initial conceptual framework for a critical analysis of cybersecurity standards in the IT/OT domain in the context of SMRs. The identified gaps and interdependencies are further refined and translated into specific security mechanisms, requirements, and research questions.

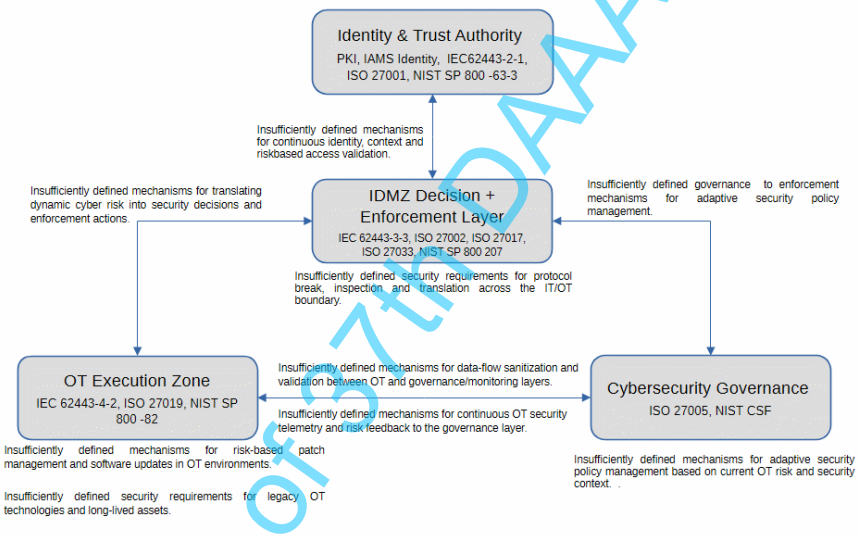

Fig. 1. Conceptual Framework for the Critical Analysis of IT/OT Security Standards in the Context of SMR [12–33].

3. Integration of IT and OT Systems

The integration of IT and OT constitutes a strategic factor influencing the safety, economic viability, and regulatory acceptability of SMR projects [25], [26]. Integrating these two technological domains enables more efficient operation and enhanced analytical capabilities [2]. At the same time, however, a greater emphasis must be placed on cybersecurity across the various technological layers [27]. In the area of IT/OT integration, a unified security architecture is necessary. This architecture incorporates network segmentation and clearly defined security zones [10], [27], mandates that interconnections between zones be implemented only through controlled interfaces and ensures the strict control and monitoring of data flows between zones [10]. Furthermore, it ensures the strict control and monitoring of data flows between zones [10] and applies the defence-in-depth principle [10], [11], [12]. This requires risk assessments to be conducted before establishing or modifying connectivity between IT and OT [12], [27]. Finally, the architecture utilizes a demilitarized zone (DMZ) between corporate and operational networks to protect systems critical to nuclear safety and to mitigate cyber threats arising from interconnection with less secure networks [11], [12], [25]. Figure 2 illustrates the proposed reference architecture for IT/OT cybersecurity in an SMR environment. The architecture is based on selected principles and requirements of the IEC 62443 and IEC 62645 standards, relevant IAEA guidelines, and NIST2 Directive recommendations. Specifically, these include security zones and communication paths, network segmentation, security boundaries, the defence-in-depth principle, and controlled data flows, which are based on NIST SP 800-82 [11], [12], [16], [18], [22], [30], [31].

Working Paper of 37th DAAAM Symposium

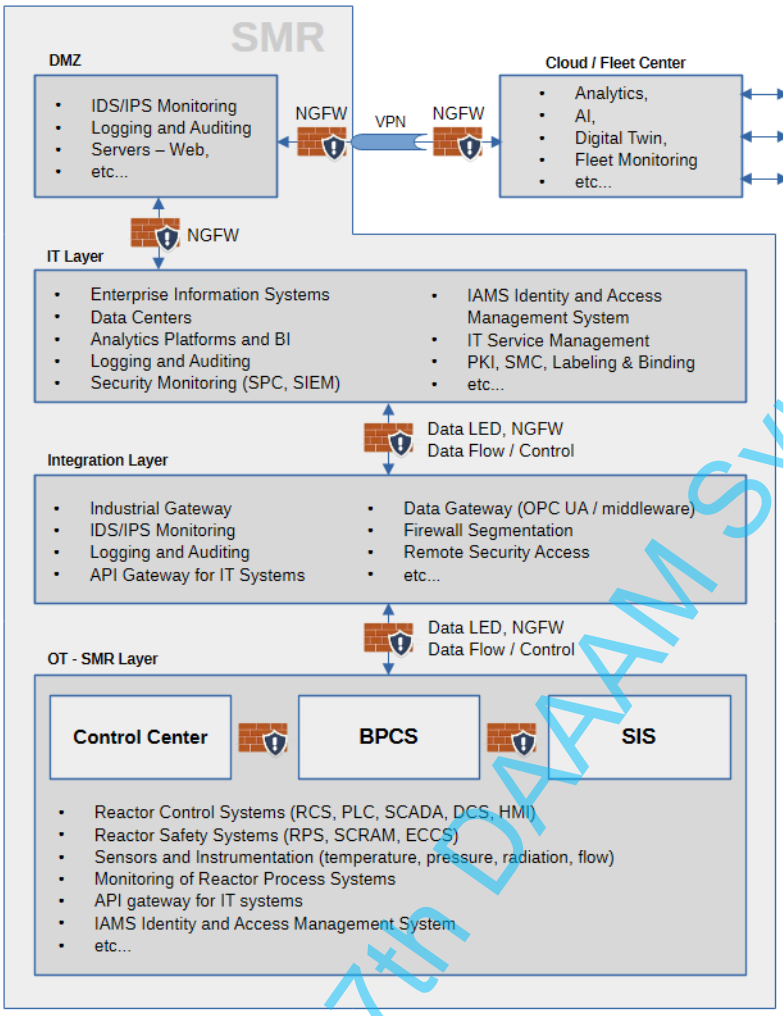

Fig. 2. Conceptual Reference Architecture for SMR IT/OT Cybersecurity [11], [12], [16], [18], [22], [30], [31].

4. Consolidated IT/OT Security Implementation Model at SMR

The proposed model defines the integration of IT and OT through unified security oversight, a common governance structure, a threat-ticketing system, and coordinated incident management [17], [21], [29]. Crucially, the framework integrates technological measures, process management, and strategic security management [17], [37]. Additional layers comprehensively address physical security, the human factor, and the convergence of safety and security considerations [17], [24], [28].

The model comprises the following base layers [11], [14], [23], [40]:

- The “Governance” layer, which establishes strategic security oversight;
- The “Safety and Security Management Processes” layer, which defines process-level management requirements;
- The “Technical Implementation” layer, which governs technological implementation.

Working Paper of 37th DAAAM Symposium

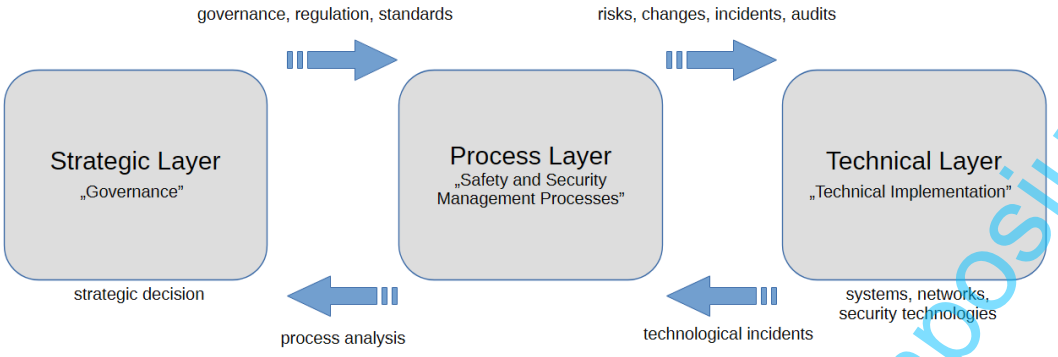

Fig. 3. Basic Classification [11], [14], [23], [40].

4.1. Governance - Strategic Layer

The strategic layer represents the highest level of security management in the SMR environment and defines the direction and principles for protecting IT/OT systems. Security is not merely a technical concern but an area that requires systematic integration into decision-making processes [10], [29], [35]. Existing standards, such as the IEC 62443 series and the recommendations of the International Atomic Energy Agency (IAEA), provide a basic framework; however, they do not fully address the unique specifics of SMRs. Although these standards establish principles and requirements for risk management, they lack a unified mechanism for their continuous, automated, and context-adaptive implementation, particularly within IT/OT architectures.

The SMR concept offers high modularity, digitalization, and the potential for remote operation. These characteristics necessitate additional processes for managing individual layers, their interconnection, and supply chain security [9], [12], [27]. Another key aspect is the integration of "Safety and Security." Traditionally, these standards have been addressed separately; however, in SMR environments, cyber incidents can directly impact physical safety and reactor control systems. The strategic layer therefore establishes a unified framework to resolve conflicts between operational safety and cyber protection, while incorporating processes for validating modern automation technologies, including artificial intelligence (AI) [2], [12], [16]. Consequently, the strategic layer ensures comprehensive, systematic, and long-term security management by integrating processes that reflect the core characteristics of SMRs, such as modularity, supply chain resilience, and safety-security convergence [9], [12], [14], [29].

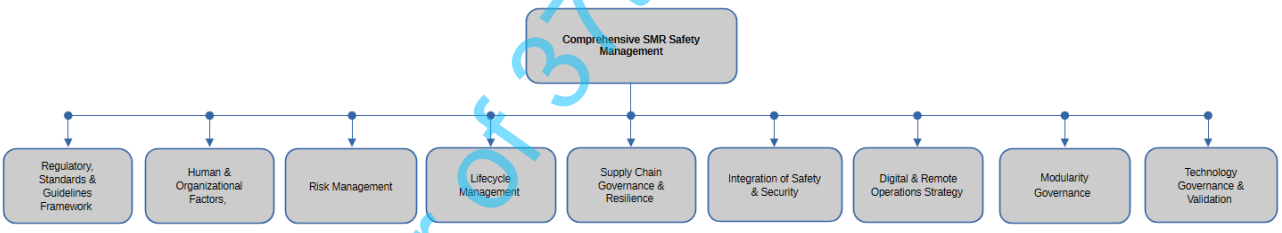

Fig. 4. Strategic Layer of Risk Security [14], [29], [36], [38].

4.2. Safety and Security Management Processes - Process Layer

The process layer is linked to an appropriate process framework [10]. Risk analysis plays a crucial role and incorporates an impact assessment that considers the innovative SMR safety concept [9], [10]. Equally important is the area of incident management, where scenarios involving cyber-attacks on I&C equipment are clearly defined; one example is the disruption of communication between systems. Effective incident management requires strict coordination among IT security, operational personnel, and emergency management [9], [14], [27], [29]. Furthermore, SMR environments necessitate robust change management, which involves thorough validation of every modification in an isolated or test environment to minimize the risk of compromising security and operational stability [14], [15], [29]. A key component of this layer is a supply chain security strategy that defines rigorous vendor screening procedures for SMR projects [1], [15].

In the context of modern SMRs, however, the process layer incorporates innovative approaches based on digitization and automation. One significant development is the use of digital twins, which enable predictive maintenance, simulation of failure scenarios, and real-time operational optimization [1], [16], [18], [22], [24]. Another promising development is the implementation of advanced autonomous security features incorporating deep learning and neural networks. These advanced technologies support the early detection of anomalies and assist operators in decision-making, while adhering to the "Human-in-the-Loop" principle [14], [16], [18].

In addition, the "Security by Design" concept is systematically promoted, encompassing "Zero Trust Architecture," network segmentation, and the integration of security measures from the earliest stages of system design [14], [15], [23],

Working Paper of 37th DAAAM Symposium

[36]. Innovation must also extend to supply chains, where advanced methods for component traceability and continuous software verification are utilized [1], [15], [23]. These approaches are tailored to reflect the context of SMR construction. Ultimately, security management evolves from isolated to integrated security measures, toward a data-driven and adaptive security management system [1], [16], [18].

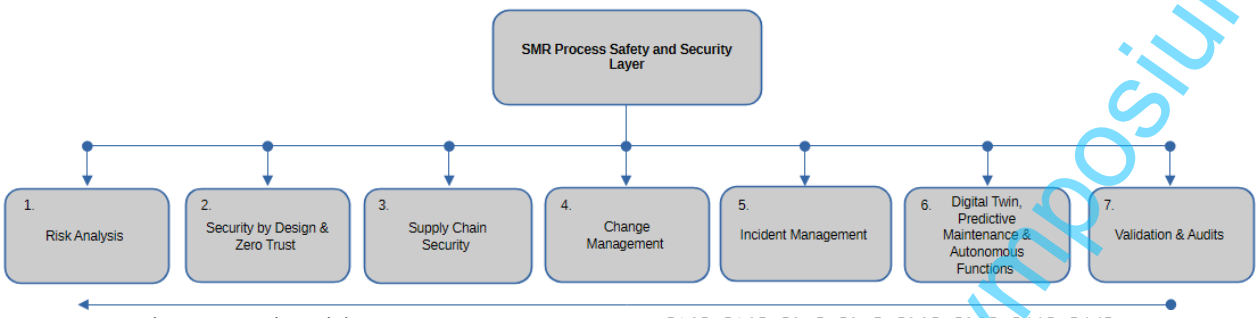

Fig. 5. Security Risk Management Process Layer [18], [19], [25], [27], [32], [39], [40], [44].

4.3. Technical Implementation - Technology Layer

The technology layer involves the implementation of specified security mechanisms and architectural principles to protect critical equipment [10]. An important element is the segmentation of systems into security zones that separate safety, instrumentation and control (I&C), and IT systems. Communication between these zones is controlled through mechanisms such as air gaps or data diodes in accordance with the "Zones and Conduits" model as defined by the International Electrotechnical Commission (IEC) 62443 series of standards [2], [15], [19], [20], [30], [39]. The protection of critical systems includes whitelist-based access control, system hardening (PLCs, DCSs, SCADA), restrictions on remote access, and appropriately implemented cryptography [10], [30], [37]. In this domain, cryptographic protection is further enhanced through post-quantum cryptography (PQC) and quantum-key distribution (QKD) mechanisms to address the future threat posed by quantum computers [45]. Monitoring and detection are ensured using intrusion prevention systems (IPSs), intrusion detection systems (IDSs), and anomaly analysis supported by a centralized security operations centre (SOC) [10], [13], [18]. Furthermore, system resilience is critical, requiring redundancy and precisely defined parameters distinguishing between fail-safe [46], [47], [48] and fail-secure behaviour [49], [50], [51]. This encompasses, for example, safe reactor shutdown modes designed to preserve the established cybersecurity mechanisms.

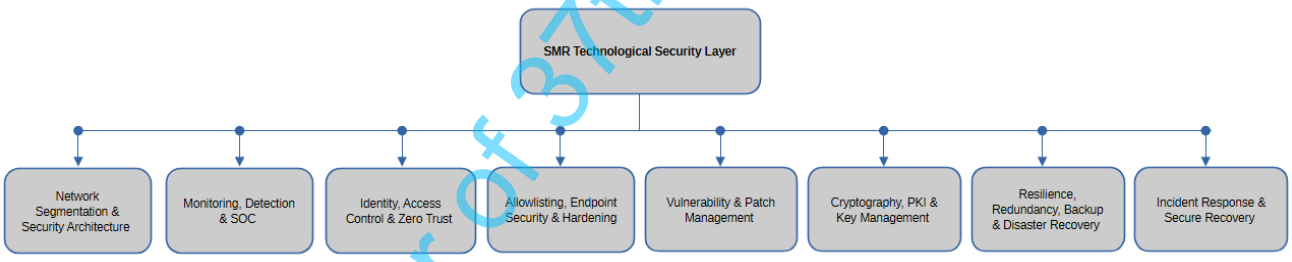

Fig. 6. Technical Security Risk Management Layer [11], [13], [18], [20], [26], [28], [31], [32], [40], [41].

5. Limitations and Future Validation

The proposed model is characterized as a preliminary conceptual framework, as it has not yet been empirically validated in an SMR operational environment. This limitation stems primarily from the current absence of a fully operational SMR suitable for practical verification of the proposed approach. Consequently, future validation will combine expert assessments with laboratory testing and simulated environments, followed by a structured pilot implementation. The evaluation framework encompasses both qualitative and quantitative criteria, specifically focusing on threat detection latency, mean time to respond, mean time to repair (MTTR), availability and recovery time of critical safety functions, and regulatory compliance mapping coverage. These metrics provide a structured foundation for assessing the completeness, usability, and practical effectiveness of the proposed model.

6. Conclusion

The digitization of SMRs represents a major technological trend that offers new opportunities for operational optimization while concurrently introducing new security challenges. The proposed consolidated IT/OT security implementation model does not involve the introduction of new, isolated security concepts but rather focuses on their systematic integration. This integration successfully establishes vital links between cybersecurity management processes

Working Paper of 37th DAAAM Symposium

and technical security measures within SMR systems. Consequently, future research will focus on validating the proposed model through targeted pilot projects in SMR operational environments. Such validation will enable the assessment of the model's functionality, reliability, and practical applicability under real-world conditions. In parallel, the model will be continuously refined to reflect rapidly evolving technological trends and dynamic regulatory requirements. The resulting insights will also be transferable to other critical infrastructure systems. An essential component of this process remains the systematic training of a new generation of experts. Developing professionals capable of bridging the gap between traditionally separate technical and non-technical disciplines is of fundamental importance for the effective implementation and long-term sustainability of integrated IT/OT security.

7. Acknowledgments

This work was supported by the Internal Grant Agency of Tomas Bata University under the project No. IGA/CebiaTech/2026/002.

8. References

[1] International Atomic Energy Agency (2024). Small Modular Reactors: Advances in SMR Developments. Available from: https://doi.org/10.61092/iaea.3o4h-svum

[2] Kharchenko, V., Shchehlov, V., Ivasiuk, O., & Morozova, O. (2026). Digital Twin-Based Lifecycle Methodology for Ensuring Safety of NPP/SMR. Technologies, 14(1), 46. ISSN 2227-7080. Available from: https://doi.org/10.3390/technologies14010046

[3] International Atomic Energy Agency (2022). Technical Meeting on Instrumentation and Control and Computer Security for Small Modular Reactors and Microreactors. Online. Available from: https://www.iaea.org/events/evt2100684

[4] International Atomic Energy Agency (2017). IAEA Nuclear Energy Series No. NP-T-3.19. Online. Available from: https://www.iaea.org/publications

[5] Eggers, S. & Anderson, R.: Cyber-Informed Engineering for Nuclear Reactor Digital Instrumentation and Control, Chapter in: Nuclear Reactors: Spacecraft Propulsion, Research Reactors, and Reactor Analysis Topics, Pope, C. L. (Ed.), pp. 95-112, IntechOpen, ISBN 978-1-83969-940-5, Available from: doi.org

[6] Ayodeji, A., Mohamed, M., Li, L., Di Buono, A., Pierce, I., et al. (2023). Cyber security in the nuclear industry: A closer look at digital control systems, networks and human factors. Progress in Nuclear Energy, 161, 104738. ISSN 0149-1970. Available from: https://doi.org/10.1016/j.pnucene.2023.104738

[7] Bhamare, D., Zolanvari, M., Erbad, A., Jain, Raj., Khan, K., et al. (2020). Cybersecurity for industrial control systems: A survey. Computers & Security, 89, 101677. ISSN 0167-4048. Available from: https://doi.org/10.1016/j.cose.2019.101677

[8] Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arabian Journal for Science and Engineering, 45(4), 3171-3189. ISSN 2193-567X. Available from: https://doi.org/10.1007/s13369-019-04319-2

[9] Computer Security of Instrumentation and Control Systems at Nuclear Facilities (2018). Online. IAEA. Available from: https://www-pub.iaea.org/MTCD/Publications/PDF/P1787_web.pdf.

[10] Computer Security Techniques for Nuclear Facilities (2021). Online. IAEA. Available from: https://www.iaea.org/publications/14729/computer-security-techniques-for-nuclear-facilities.

[11] Locatelli, G., Bingham, C., & Mancini, M. (2014). Small modular reactors: A comprehensive overview of their economics and strategic aspects. Progress in Nuclear Energy, 73, 75-85. ISSN 0149-1970. Available from: https://doi.org/10.1016/j.pnucene.2014.01.010

[12] International Atomic Energy Agency (2011). Computer Security at Nuclear Facilities. Online. Available from: https://www.iaea.org/publications/8691/computer-security-at-nuclear-facilities

[13] OECD Nuclear Energy Agency (2022). Consensus Position on the Impact of Cyber Security Features on Digital Instrumentation and Control Systems Important to Safety at Nuclear Power Plants [CP-08]. Online. Available from: https://www.oecd-nea.org/jcms/pl_75241/consensus-position-on-the-impact-of-cyber-security-features-on-digital-instrumentation-and-control-systems-important-to-safety-at-nuclear-power-plants-cp-08?details=true

[14] Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). Guide to Industrial Control Systems (ICS) Security: NIST SP 800-82 Rev. 2. Online. (Withdrawn and superseded by NIST SP 800-82r3 in 2023). Available from: https://doi.org/10.6028/nist.sp.800-82r2

[15] International Electrotechnical Commission (2007). Industrial communication networks – Network and system security: IEC 62443. Geneva: IEC, 1st edition.

Working Paper of 37th DAAAM Symposium

[16] Daniell, J., Kobayashi, K., Alajo, A., & Alam, S. B. (2025). Digital twin-centered hybrid data-driven multi-stage deep learning framework for enhanced nuclear reactor power prediction. Energy and AI, 19, 100450. ISSN 2666-5468. Available from: https://doi.org/10.1016/j.egyai.2024.100450

[17] International Atomic Energy Agency (2024). New CRP: Enhancing Computer Security of Small Modular Reactors and Microreactors. Online. Available from: https://www.iaea.org/newscenter/news/new-crp-enhancing-computer-security-of-small-modular-reactors-and-microreactors

[18] Mondal, K., Martinez, O., & Jain, P. (2024). Advanced manufacturing and digital twin technology for nuclear energy. Frontiers in Energy Research, 12, Article 1339836. ISSN 2296-598X. Available from: https://doi.org/10.3389/fenrg.2024.1339836

[19] Czech Standardization Agency (2025). Security for industrial automation and control systems – Part 2-1: Security program requirements for IACS asset owners: ČSN EN IEC 62443-2-1. Current edition. (In Czech).

[20] Czech Standardization Agency (2019). Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components: ČSN EN IEC 62443-4-2. Current edition. (In Czech).

[21] U.S. Department of Energy Office of Scientific and Technical Information (2025). Managing Cybersecurity in Small Modular Reactors: Strategies for Addressing Modularity, Cloud, and Remote Operation Risks. Online. Available from: https://www.osti.gov/servlets/purl/2588291

[22] Yu, H. (2025). A digital twin-based system for full-lifecycle safety management and dynamic risk assessment in nuclear power plants. Discover Artificial Intelligence, 5, 356. ISSN 2731-0809. Available from: https://doi.org/10.1007/s44163-025-00618-w

[23] OECD Nuclear Energy Agency (2021). Digital transformation: Opportunities and challenges for the nuclear sector. Online. Available from: https://www.oecd-nea.org/jcms/pl_59100/digital-transformation-opportunities-and-challenges-for-the-nuclear-sector

[24] Huang, Q., Zeng, W., Liu, Jia., Zhang, Z., Deng, J., et al. (2025). Shaping the future of nuclear reactors with digital twins: Current developments and perspectives. Applied Energy, 402, 126922. ISSN 0306-2619. Available from: https://doi.org/10.1016/j.apenergy.2025.126922

[25] Czech Standardization Agency (2018). Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation: ČSN EN ISO/IEC 27004. Current edition. (In Czech).

[26] Czech Standardization Agency (2017). Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services: ČSN EN ISO/IEC 27017. Current edition. (In Czech).

[27] Czech Standardization Agency (2023). Information security, cybersecurity and privacy protection – Guidance on managing information security risks: ČSN EN ISO/IEC 27005. Current edition. (In Czech).

[28] Czech Standardization Agency (2020). Information technology – Security techniques – Information security controls for the energy utility industry: ČSN EN ISO/IEC 27019. Current edition. (In Czech).

[29] Czech Standardization Agency (2023). Information security, cybersecurity and privacy protection – Information security management systems – Requirements: ČSN ISO/IEC 27001. Current edition. (In Czech).

[30] Czech Standardization Agency (2021). Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design: ČSN EN IEC 62443-3-2. Current edition. (In Czech).

[31] Czech Standardization Agency (2016). Information technology – Security techniques – Network security – Part 1: Overview and concepts: ČSN EN ISO/IEC 27033-1. Current edition. (In Czech).

[32] Czech Standardization Agency (2023). Information security, cybersecurity and privacy protection – Information security controls: ČSN EN ISO/IEC 27002. Current edition. (In Czech).

[33] Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). Digital identity guidelines: NIST SP 800-63-3. Online. Available from: https://doi.org/10.6028/nist.sp.800-63-3

[34] National Institute of Standards and Technology (2024). The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Papers (CSWP). Online. Available from: https://doi.org/10.6028/nist.cswp.29

[35] Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023). Guide to Operational Technology (OT) security: NIST SP 800-82r3. Online. Available from: https://doi.org/10.6028/nist.sp.800-82r3

[36] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture: NIST SP 800-207. Online. Available from: https://doi.org/10.6028/nist.sp.800-207

[37] SSH Academy (2025). Critical Infrastructure Cybersecurity: Key Concepts Explained. Online. Available from: https://www.ssh.com/academy/operational-technology/critical-infrastructure-cybersecurity-key-concepts-explained

Working Paper of 37th DAAAM Symposium

[38] International Atomic Energy Agency (2020). Advances in Small Modular Reactor Technology Developments. Online. Available from: https://aris.iaea.org/Publications/SMR_Book_2020.pdf

[39] Czech Standardization Agency (2019). Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels: ČSN EN IEC 62443-3-3. Current edition. (In Czech).

[40] International Atomic Energy Agency (2025). Considerations for Deploying Artificial Intelligence Applications in the Nuclear Power Industry. IAEA Nuclear Energy Series. ISBN 9789201155252. ISSN 1995-7807. Available from: https://doi.org/10.61092/iaea.s6uy-wjt8

[41] Kapoor, S., Kumar, S., & Vardhan, H. (2025). Cyber security of OT networks: A tutorial and overview. Cornell University. Online. Available from: https://arxiv.org/abs/2502.14017

[42] Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). Guide to Industrial Control Systems (ICS) Security: NIST SP 800-82 Rev. 2. Online. (Withdrawn and superseded by NIST SP 800-82r3 in 2023). Available from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[43] Czech Standardization Agency (2021). Information security, cybersecurity and privacy protection – Governance of information security: ČSN EN ISO/IEC 27014. Current edition. (In Czech).

[44] Czech Standardization Agency (2024). Information technology – Information security incident management – Part 1: Principles and process: ČSN EN ISO/IEC 27035-1. Current edition. (In Czech).

[45] Moric, Z., Milovec, M., & Petrunic, R. (2024). Application of Quantum Cryptography in Securing Network Communications. Proceedings of the 35th DAAAM International Symposium, pp. 0055-0064, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-44-0, ISSN 1726-9679, Vienna, Austria. Available from: https://doi.org/10.2507/35th.daaam.proceedings.008

[46] Czech Standardization Agency (2013). Nuclear power plants – Instrumentation and control important to safety – General requirements for systems: ČSN EN 61513. Current edition. (In Czech).

[47] Czech Standardization Agency (2010). Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements: ČSN EN 61508-1 ed. 2. Current edition. (In Czech).

[48] International Atomic Energy Agency: Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), IAEA, Vienna, 2016, ISBN 978-92-0-109315-8

[49] Czech Standardization Agency (2021). Nuclear power plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity: ČSN EN IEC 62859. Current edition. (In Czech).

[50] Ross, R., Winstead, M., & McEvilley, M. (2022). Engineering Trustworthy Secure Systems: NIST Special Publication 800-160 Vol. 1 Rev. 1. National Institute of Standards and Technology. Online. Available from: https://csrc.nist.gov/pubs/sp/800/160/v1/r1/final

[51] Joint Task Force (2020). Security and Privacy Controls for Information Systems and Organizations: NIST Special Publication 800-53 Rev. 5. National Institute of Standards and Technology. (Include updates as of August 2025, Release 5.2.0). Online. Available from: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Working Paper of 37th DAAAM Symposium