A Study on Cybersecurity Implementation Activities and Considerations for Security-by-Design in Small Modular Reactors (SMRs)

Jae-Gu Song[a]*, Jaekwan Park[a], Young-Jun Lee[a], Yonggu Lee[a], Seongyeol Oh[a], Inhye Hahm[a], Juhyung Song[a]
[a] *Korea Atomic Energy Research Institute, Daejeon, South Korea*
[*]*Corresponding author: jgsong@kaeri.re.kr*

Keywords : Security-by-Design (SbD), Cybersecurity, Small Modular Reactors (SMRs), Lifecycle Security, Nuclear Regulatory Framework

1. Introduction

As cyber threats continue to evolve, the necessity for robust cybersecurity measures in critical infrastructure, including nuclear facilities, has become more urgent than ever. Traditional approaches that emphasize physical protection and post-incident response are no longer sufficient to address modern, complex cyber risks. In this context, the concept of Security-by-Design (SbD)—which integrates cybersecurity from the earliest stages of system planning and design through to operation and decommissioning—has emerged as a global imperative [1,3].

Internationally, standards and guides such as those from the IAEA and IEC emphasize a lifecycle-based cybersecurity approach to ensure consistent protection from design to decommissioning [1,2,3,4]. In South Korea, the implementation of cybersecurity at nuclear facilities is inspected in accordance with the technical standards outlined in KINAC RS-015 [5], which serves as the regulatory basis for nuclear cybersecurity. However, since cybersecurity regulations were only formalized in the late 2010s, associated reviews and implementation efforts have primarily occurred during the operational phase of nuclear power plants. Consequently, cybersecurity considerations have often been introduced after the completion of system design, which has limited the extent to which security measures could be inherently embedded into the system architecture. As a result, the application of technical cybersecurity controls has faced practical constraints, leading to increased reliance on physical protection measures and administrative or operational compensatory controls to manage residual risks. This timing has posed practical challenges for integrating cybersecurity into the foundational design and has reduced the overall effectiveness of threat mitigation.

To address these limitations, recent efforts in South Korea are focused on establishing a legal and regulatory framework that enables the application of cybersecurity requirements from the early stages of system development. This shift is particularly relevant in the context of Small Modular Reactor (SMR) projects, where the adoption of Security-by-Design (SbD) principles from the outset is increasingly recognized as essential for ensuring resilient and future-proof nuclear systems, in alignment with international guidance.

This study investigates the essential requirements for applying SbD to Small Modular Reactors (SMRs) by analyzing current regulatory and technological trends. With international and domestic guidance increasingly emphasizing life-cycle-based cybersecurity, there is a growing need to redefine regulatory and implementation strategies to ensure that cybersecurity becomes an integral part of the early design process, rather than a reactive measure.

In particular, harmonizing SbD with existing safety requirements, defining its application scope in early design phases, and developing integrated regulatory strategies are key considerations. This paper aims to identify the regulatory and technical elements necessary for effective SbD implementation in SMRs and to provide strategic insights that can guide future improvements in cybersecurity governance and regulatory practice.

2. Trends in Guideline-Based Approaches to Security-by-Design for Nuclear Facilities

This section reviews key international and domestic guidelines that inform Security-by-Design (SbD) implementation in nuclear facilities. By analyzing the structure and emphasis of each guide, we identify essential considerations for incorporating cybersecurity throughout the system lifecycle.

2.1 IEC 62645:2019 [1]

IEC 62645 is an international standard that specifies cybersecurity requirements for protecting digital instrumentation and control (I&C) systems in nuclear power plants against malicious cyberattacks. One of its key features is the incorporation of a lifecycle-based security management framework tailored to the nuclear domain, emphasizing the continuous application of security controls from the design stage through to system retirement.

Key requirements include:

- Risk assessment and the development of a security design plan during the design phase,
- Control of communication paths and wireless devices,
- Establishment of security zones,
- Verification and validation testing of security functions during the integration and verification phase,

- Periodic security audits and configuration management during operation,
- Dynamic responses to emerging threats, and
- Protection and secure disposal of sensitive data at the retirement phase.

It emphasizes the importance of implementing Security-by-Design (SbD) principles throughout the full lifecycle of nuclear I&C systems, recognizing the critical link between cybersecurity and overall safety in nuclear facilities.

2.2 IEC 63096:2020 [2]

IEC 63096:2020 extends the framework of IEC 62645 by offering a structured and detailed set of security controls tailored for digital I&C systems in nuclear facilities. Reflecting a Security-by-Design (SbD) philosophy, this standard emphasizes the proactive integration of cybersecurity controls across the entire lifecycle of a system—from initial design through operation to retirement.

As part of the SbD trend, IEC 63096 defines security controls that are:

- Mapped to specific security levels (S1–S3) based on system criticality,
- Aligned with distinct lifecycle stages such as design, development, installation, operation, maintenance, and decommissioning,
- Oriented around security objectives including prevention, detection, and correction.

By structuring security requirements along these dimensions, IEC 63096 ensures that cybersecurity is treated not as a supplementary consideration but as a core, evolving component of system engineering [2,6].

2.3 IAEA NSS No. 17-T (Rev.1) [3]

The IAEA NSS No. 17-T (Rev.1) provides a comprehensive risk-informed framework for developing computer security programs and defensive computer security architectures (DCSA) to protect Sensitive Digital Assets (SDAs) within nuclear facilities. Recognizing cybersecurity as an integral part of nuclear security, the document outlines technical and procedural requirements aimed at mitigating threats such as physical sabotage, data leakage, and operational disruption caused by cyberattacks.

Reflecting a Security-by-Design (SbD) approach, the guideline mandates the consistent integration of computer security across all lifecycle phases—from planning and design to decommissioning. Security is not treated as a discrete technical feature, but as a coordinated effort involving Computer Security Programmes (CSP) and Computer Security Risk Management (CSRM).

Key lifecycle-based SbD requirements include:

- Planning: Establishment of a facility-wide CSRM strategy, early DCSA development, and protection of sensitive documentation during external collaborations.
- Construction: Prioritization of physical security installations before SDA deployment and supply chain integrity management.
- Commissioning: Inclusion of security validation steps during FAT/SAT, such as disabling default accounts and testing security features.
- Operations: Role-based access control, regular log reviews, and adherence to CSP/DCSA policies based on the system's security level.
- Maintenance: Implementation of compensating controls during temporary security function disablement, and strict controls for portable and remote maintenance tools.
- Cessation: Security reassessment in response to system or personnel changes, with safe handling and removal of SDAs.
- Decommissioning: Secure data destruction of retired SDAs and continued risk analysis for remaining connected systems.

This document reinforces the principle that effective SbD in nuclear facilities requires cross-functional stakeholder involvement and continuous security validation throughout the system lifecycle [3,7].

2.4 Guidelines for Security by Design Across the Lifecycle of National Nuclear Facilities [4]

Issued by South Korea's National Intelligence Service (NIS), the "Guidelines for Security by Design Across the Lifecycle of National Nuclear Facilities" provides a structured policy framework to implement Security-by-Design (SbD) in alignment with international standards. It establishes baseline cybersecurity practices to be consistently applied from system planning to decommissioning, aiming to proactively mitigate evolving cyber threats.

In this context, SbD is defined as the integration of cybersecurity measures—driven by risk assessments—throughout all lifecycle phases, including planning, design, implementation, testing, operation, and retirement, to systematically eliminate system vulnerabilities.

The guideline presents 16 foundational principles for SbD, covering security governance, procedural controls, risk analysis, defense-in-depth, secure architecture and network separation, cyber threat intelligence, continuous monitoring, regulatory and standards compliance, security training, human and supply chain security, zero-trust practices, operational continuity, incident response, and protection against physical and environmental risks.

Furthermore, it specifies the minimum cybersecurity activities required for each lifecycle stage—Planning, Design, Implementation, Testing, Installation, Operation, Decommissioning—to ensure proactive and integrated security management across all phases of nuclear facility operations.

3. Cybersecurity Implementation Activities and Security-by-Design Considerations Across the SMR Lifecycle

This section outlines key Security-by-Design (SbD) considerations and corresponding activities that should be implemented throughout the lifecycle of Small Modular Reactors (SMRs). Drawing on international standards such as IEC 63096 and national guidelines such as Korea's lifecycle-based SbD framework, the analysis identifies essential cybersecurity integration points across each lifecycle phase—from planning to decommissioning.

International standards and guidance documents, including those from the IEC and IAEA, consistently emphasize the importance of applying cybersecurity measures across the entire system lifecycle as a core principle of SbD. Rather than treating cybersecurity as a discrete task or a post-design activity, these frameworks advocate for proactive integration of security from the earliest phases of planning and design, continuing through implementation, operation, and eventual decommissioning. This lifecycle-based approach ensures that security requirements are not only technically sound but also systematically aligned with evolving threats and operational realities over time.

In line with this global trend, SMRs—due to their modularity, advanced digitalization, and potential for wide deployment—require rigorous lifecycle-based cybersecurity planning to ensure secure and resilient operation in diverse environments.

- Planning Phase : At this stage, foundational SbD strategies are established. Activities include defining security objectives, identifying potential cyber risks, and integrating security planning into the overall project strategy. Roles and responsibilities related to cybersecurity are assigned, and key digital assets are preliminarily identified for further assessment.
- Design Phase : This phase focuses on embedding security requirements into the architectural design. Key considerations include developing a defense-in-depth architecture, mapping security controls to system security levels, and designing appropriate isolation and access mechanisms. Interactions between safety and security functions are also analyzed to ensure compatibility and avoid conflicts.
- Implementation Phase : During implementation, designed security features are realized. This includes integrating access controls, authentication mechanisms, and secure communication pathways. Additionally, third-party components and supply chain elements are reviewed for compliance with security requirements, ensuring integrity and traceability throughout system assembly.
- Integration & Verification Phase : Security features undergo functional testing and validation. Vulnerability assessments are performed, and the effectiveness of implemented controls is evaluated. This stage also includes the analysis of security-safety interactions and the verification that no unintended consequences arise from security measures. In particular, verification and validation (V&V) activities—traditionally focused on safety systems—may need to be carefully extended to interface with cybersecurity functions. It is advisable to consider coordinated planning so that cybersecurity verification efforts can align with existing V&V frameworks. This approach can help identify potential interactions, overlaps, or conflicts between safety and security implementations, thereby contributing to more integrated and reliable system validation.
- Installation Phase : In the installation phase, the secure configuration of systems is validated in the actual operating environment. SbD activities include activating security settings, protecting sensitive interfaces, and applying protective measures for physical components. Secure deployment practices are critical to avoid exposing systems to vulnerabilities during transition.
- Operation & Maintenance Phase : Continuous security monitoring, patch management, and change control processes are emphasized. Any system modifications must be preceded by security impact assessments. Remote access tools and maintenance devices—especially those increasingly considered in SMR designs for remote monitoring and support—must be managed under strict control and auditing mechanisms to mitigate potential threats during ongoing operations.
- Decommissioning Phase : Security considerations extend through the final phase of the lifecycle. Sensitive or critical digital assets are securely erased or physically destroyed, and residual cybersecurity risks are assessed and mitigated. Secure deactivation of access credentials and network interfaces is critical to prevent post-operation exploitation.

4. Conclusions

As the i-SMR project is currently progressing through the design stages, the integration of Security-by-Design (SbD) principles is particularly critical to ensure that cybersecurity considerations are embedded early and consistently throughout the system's lifecycle. This study reviewed key international standards and domestic guidelines related to SbD and identified essential security activities applicable to each phase of an SMR's lifecycle.

During the design stage, it is essential to proactively address security requirements such as establishing a risk-based defensive architecture, defining system-level security controls, and planning for potential interactions between safety and security functions. It is also important to identify critical digital assets, define security roles and responsibilities, and secure the development environment from external threats.

Implementing these SbD strategies during the design phase will provide a strong foundation for secure development and facilitate smoother regulatory

engagement in subsequent stages. As the i-SMR advances toward implementation, the early incorporation of cybersecurity will enhance the system's resilience and ensure compliance with both domestic and international expectations.

ACKNOWLEDGMENTS

This paper was supported by the Nuclear Safety Research Program through the Regulatory Research Management Agency for SMRS (RMAS) and the Nuclear Safety and Security Commission (NSSC) of the Republic of Korea (No. 1500-1501-409).

REFERENCES

[1] IEC 62645:2019, Nuclear power plants – Instrumentation and control systems – Requirements for security programmes for computer-based systems, International Electrotechnical Commission, 2019.
[2] IEC 63096:2020, Nuclear facilities – Instrumentation and control systems – Security controls, International Electrotechnical Commission, 2020.
[3] IAEA Nuclear Security Series No. 17-T (Rev. 1), Computer Security at Nuclear Facilities: Implementing Guide, International Atomic Energy Agency, Vienna, 2021.
[4] National Intelligence Service, Guidelines for Security-by-Design Across the Lifecycle of National Nuclear Facilities, Republic of Korea, December 2024.
[5] KINAC/RS-015 rev.02, Cybersecurity Technical Requirements for Nuclear Facilities, Korea Institute of Nuclear Nonproliferation and Control (KINAC), 2023.
[6] ANSI/ISA 62443-4-1:2018, Security for Industrial Automation and Control Systems – Part 4-1: Secure Product Development Lifecycle Requirements, International Society of Automation, 2018.
[7] IAEA Nuclear Security Series No. 33-T, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, International Atomic Energy Agency, Vienna, 2018.