International Trends in Lifecycle-Based Cybersecurity Regulation for Nuclear Facilities

Yonggu Lee[a*], Seongyeol Oh[a], Ju Hyung Song[a], Joonseok Lim[b], Gyunyoung Heo[b]
[a]*Korea Atomic Energy Research Institute, Daejeon, South Korea*
[b]*Kyung Hee University, Yongin, South Korea*
[*]*Corresponding author: ygl@kaeri.re.kr*

***Keywords** **:** Lifecycle, Cybersecurity, Nuclear Facilities, Regulatory Framework, Graded Approach

1. Introduction

With the growing reliance of nuclear facilities on digital instrumentation and control (I&C) and information systems, cyberattacks have emerged as a serious threat to safety, security, and emergency preparedness (SSEP) functions. Moreover, vulnerabilities introduced at the design phase may remain latent throughout the subsequent operation and decommissioning phases, implying that cyber threats are not confined to any single phase but extend across the entire lifecycle of a nuclear facility.

Reflecting this trend, international guidance and standards recommend that cybersecurity should be applied in an integrated manner across the entire lifecycle of nuclear facilities. The International Atomic Energy Agency (IAEA) provides non-binding technical guidance on lifecycle computer security [1,2], and IEC 62645:2019 [3], a voluntary international standard that becomes mandatory only when incorporated into national regulations or licensing bases, specifies security requirements for I&C programmable digital systems throughout the system lifecycle. In South Korea, although the legal basis for the security by design of nuclear facilities has been established, detailed technical requirements for lifecycle cybersecurity still need to be developed. In addition, since the characteristics and risk levels differ across facility types, uniformly applying identical lifecycle cybersecurity regulations to all facilities may be inefficient. It is thus necessary to examine the regulatory practices of leading nuclear countries regarding lifecycle cybersecurity.

Against this backdrop, this study surveys the lifecycle cybersecurity regulatory frameworks of the IAEA and major regulatory bodies, namely the U.S. Nuclear Regulatory Commission (NRC), the Canadian Nuclear Safety Commission (CNSC), and the U.K. Office for Nuclear Regulation (ONR). The analysis covers five facility types (large power reactors, research reactors, fuel cycle facilities, radioactive waste management facilities, and irradiation facilities), focusing on the regulatory frameworks and key regulatory features of lifecycle cybersecurity. Based on the survey results, this study identifies overall trends in lifecycle cybersecurity regulation, which are expected to serve as a basis for a subsequent gap analysis.

2. Regulatory Trends on Lifecycle Cybersecurity for Nuclear Facilities

In this section, the lifecycle cybersecurity regulatory frameworks of the IAEA, the NRC, the CNSC, and the ONR are examined, focusing on the hierarchy of regulatory documents, the key features of regulations across facility types, and the coverage of lifecycle phases.

2.1 IAEA

Since the publication of NSS 17 (Computer Security at Nuclear Facilities) in 2011, the IAEA has developed a hierarchical set of computer security guidance documents. Although not legally binding, the NSS guides have become the international basis for nuclear cybersecurity. Among them, NSS 17-T Rev.1 divides the facility lifecycle into eight phases, namely planning, siting, design, construction, commissioning, operations, cessation of operations, and decommissioning, and provides computer security guidance for each phase [1]. In parallel, NSS 33-T structures the lifecycle of I&C systems and recommends verification and validation at each stage, complementing the facility lifecycle of NSS 17-T [2].

The IAEA guidance regards computer security as an attribute that should be consistently maintained throughout the lifecycle of facilities and systems, which is embodied in the following key principles: 1) secure by design, which calls for facility-level computer security risk management (CSRM) and a defensive computer security architecture (DCSA) to be established from the planning and design phases, 2) a graded approach and defense-in-depth, and 3) the continuity of the security regime through the cessation of operations and decommissioning [1].

2.2 U.S. NRC

Through the Cyber Security Roadmap (SECY-17-0034 [4]), the NRC categorized its licensees into six groups (operating power reactors, decommissioning power reactors, non-power reactors, fuel cycle facilities, independent spent fuel storage installations (ISFSIs), and byproduct materials licensees (including irradiation facilities)) and performed cybersecurity assessments for each group. For operating power reactors, 10 CFR 73.54 [5] requires licensees to establish and implement a cyber security plan (CSP) to protect SSEP functions against cyberattacks, up to and including the design basis threat (DBT). This binding rule is supported by non-binding guidance that describes acceptable implementation methods, namely regulatory guides such as RG 5.71 [6] and NRC-endorsed industry guidance such as NEI 08-09,

and the requirements are reflected throughout the licensing processes under 10 CFR Part 50 and Part 52.

In contrast, no dedicated cybersecurity regulations currently exist for the other facility types: non-power reactor (i.e., research reactor) licensees are exempted from the cyber adversary attribute of the DBT and rely on voluntary effective practices; the rule for fuel cycle facilities (10 CFR 73.53, with its draft guide DG-5062) remains at the proposed-rule stage and has not been promulgated; and ISFSIs and byproduct materials licensees are governed by their respective physical protection requirements, complemented by voluntary practices.

As a key regulatory trend regarding the decommissioning phase of power reactors, the NRC staff has submitted a final rule to the Commission (SECY-24-0011 [7]), not yet published, that would codify risk-informed termination criteria. Under this rule, the requirements of 10 CFR 73.54 would continue to apply after a licensee enters decommissioning until the fuel in the spent fuel pool has decayed sufficiently that it would not reach ignition temperature within 10 hours after a complete loss of cooling water. Once promulgated, this would extend cybersecurity requirements into the decommissioning phase with an explicit, risk-informed endpoint.

2.3 Canadian CNSC

The CNSC regulatory framework consists of four tiers, namely the Nuclear Safety and Control Act, regulations, CSA standards, and REGDOCs, and takes an integrated structure in which common regulations apply to all facilities while the stringency of obligations is graded by nuclear material category and risk level. Of these tiers, the Act and the regulations are legally binding, whereas CSA standards and REGDOCs become enforceable only when incorporated into the licensing basis through license conditions. The scope of CSA N290.7 was expanded from power reactors (2014) to nuclear facilities in general (CSA N290.7:21 [8]), and the CNSC adopted the Nuclear Security Regulations (SOR/2025-219 [9]) in 2025. SOR/2025-219 requires license applicants to submit a nuclear security plan (NSP) including a cybersecurity program, together with a threat and risk assessment (TRA). In addition, Part 2 of the regulations applies to high-security sites (HSS) such as power reactors, and Part 3 to non-HSS facilities such as research reactors, whereas Class II irradiation facilities fall outside the scope of the regulations.

With respect to the post-operational phase, SOR/2025-219 requires the licensee to protect the sensitive information identified in its TRA (section 17), where sensitive information is defined to include the prescribed information referred to in section 21 of the General Nuclear Safety and Control Regulations (GNSCR) [10]. In addition, records required under the Act, the regulations, or the license must, unless another retention period is specified, be retained until one year after the expiry of the license (GNSCR, section 28). Thus, while the cybersecurity program itself is tied to the license, record-retention obligations extend beyond license expiry, which indicates that information-related obligations are not confined to the operational phase of the facility.

2.4 U.K. ONR

The ONR regulates nuclear security under a single framework without distinguishing facility types. The Nuclear Industries Security Regulations (NISR 2003) [11] require each nuclear premises to maintain a nuclear site security plan (NSSP) encompassing physical protection, cybersecurity, and the protection of sensitive nuclear information (SNI). The Security Assessment Principles (SyAPs) [12] do not themselves impose legal obligations; they set out the principles that ONR inspectors use to form regulatory judgements when assessing dutyholder submissions required under NISR 2003, and Fundamental Security Principle 7 addresses cyber security and information assurance. Security requirements are graded according to the nuclear material category, sabotage consequences, SNI sensitivity, and the DBT. Separately from this grading of requirements, the ONR adjusts the intensity of its regulatory oversight through Regulatory Attention Levels (RALs), which are assigned on the basis of the ONR's assessment of each dutyholder's overall performance rather than the risk category of the facility.

From a lifecycle perspective, the SyAPs set out the regulatory expectation that decommissioning security be considered from all preceding lifecycle phases, including the design phase, where the Generic Design Assessment (GDA) reviews whether cyber protection is embedded in the design. As decommissioning proceeds and nuclear material is removed, the NSSP is progressively reduced and eventually withdrawn under Regulation 6. However, the SNI protection duty under Regulation 22 persists where SNI remains and applies to any entity handling SNI, so that the scope of regulation is defined by the handling of sensitive information rather than by the possession of nuclear material.

3. Conclusions

This paper examined the regulatory trends of the IAEA and major countries regarding lifecycle cybersecurity for nuclear facilities. The review indicated that the NRC maintains separate regulatory frameworks for each facility type, centered on power reactors, whereas the CNSC and the ONR apply a consistent framework to all facilities and differentiate requirements through a graded approach based on the nuclear material category and risk level. From a lifecycle perspective, cybersecurity requirements are increasingly extended to remain applicable beyond the cessation of operations. The NRC is codifying risk-informed termination criteria for the decommissioning phase, the CNSC extends record-retention obligations beyond license expiry, and the ONR expects decommissioning security planning from

the design phase with the stepwise reduction of the security plan. These trends suggest that risk-informed differentiation across facility types and explicit criteria for the relaxation and termination of requirements in the cessation and decommissioning phases are emerging as common directions in lifecycle cybersecurity regulation. Detailed gap analyses of these regulations by facility type and lifecycle phase will be conducted in subsequent studies.

ACKNOWLEDGMENTS

This work was supported by the Nuclear Safety Research Program through the Korea Foundation of Nuclear Safety (KoFONS) using the financial resource granted by the Nuclear Safety and Security Commission (NSSC) of the Republic of Korea (RS-2026-25537788).

REFERENCES

[1] International Atomic Energy Agency, Computer Security Techniques for Nuclear Facilities, IAEA Nuclear Security Series No. 17-T (Rev.1). Vienna, Austria: IAEA, 2021.
[2] International Atomic Energy Agency, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T. Vienna, Austria: IAEA, 2018.
[3] International Electrotechnical Commission, Nuclear Power Plants—Instrumentation, Control and Electrical Power Systems—Cybersecurity Requirements, IEC 62645:2019, 2nd ed., 2019.
[4] U.S. Nuclear Regulatory Commission, Update to the U.S. Nuclear Regulatory Commission Cyber Security Roadmap, SECY-17-0034, Washington, DC, USA, Feb. 28, 2017.
[5] U.S. Nuclear Regulatory Commission, “Protection of digital computer and communication systems and networks,” Title 10, Code of Federal Regulations, § 73.54.
[6] U.S. Nuclear Regulatory Commission, Cyber Security Programs for Nuclear Power Reactors, Regulatory Guide 5.71, Rev. 1, Washington, DC, USA, Feb. 2023.
[7] U.S. Nuclear Regulatory Commission, Final Rule: Regulatory Improvements for Production and Utilization Facilities Transitioning to Decommissioning, SECY-24-0011, Washington, DC, USA, 2024.
[8] CSA Group, Cyber Security for Nuclear Facilities, CSA N290.7:21, 2nd ed., 2021.
[9] Government of Canada, Nuclear Security Regulations, SOR/2025-219, Oct. 30, 2025.
[10] Government of Canada, General Nuclear Safety and Control Regulations, SOR/2000-202.
[11] United Kingdom, The Nuclear Industries Security Regulations 2003, S.I. 2003/403, 2003.
[12] Office for Nuclear Regulation, Security Assessment Principles for the Civil Nuclear Industry (SyAPs), 2022 Edition, Version 1, 2022.