# A Study on Cybersecurity Regulatory Trends for Remote Operation of Small Modular Reactors

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

***Keywords** : Cybersecurity, Remote Operation, Small Modular Reactors, Regulatory Trends

## 1. Introduction

With the global expansion of Small Modular Reactors (SMRs), operational concepts distinct from those of conventional large reactors are being actively considered, including multi module deployment and remote or distributed siting. In this context, remote operation technology, in which multiple modules are monitored and controlled from a single remote control center, has emerged as a key enabler for the deployment of SMRs in terms of economic viability and efficiency. However, remote operation presupposes the transmission of monitoring and control data across the site boundary, weakening the physical isolation based protection concept and introducing new attack surfaces such as remote access paths and wired/wireless communication networks. Ensuring cybersecurity is thus an essential prerequisite for its application.

Under the current regulatory frameworks, the U.S. Nuclear Regulatory Commission (NRC) and the Canadian Nuclear Safety Commission (CNSC) strictly limit remote access to safety systems, effectively restricting remote operation. Nevertheless, the NRC has progressively established a regulatory basis for remote operation, from the ground rules on its regulatory feasibility [1] to the performance based framework of 10 CFR Part 53 [2] and Regulatory Guide (RG) 5.96 [3], while the CNSC addresses remote access requirements based on a graded approach centered on CSA (Canadian Standards Association) N290.7 [4]. In contrast, the Korean regulatory framework, represented by RS-015 [5] of the Korea Institute of Nuclear Nonproliferation and Control (KINAC), has been developed on the premise of closed on-site networks. The introduction of remote operation would therefore require additional regulatory considerations. Against this backdrop, this study analyzes these trends to derive key considerations for a regulatory framework for Korean SMRs, including the innovative SMR (i-SMR).

## 2. Regulatory and Standardization Trends on Cybersecurity for Remote Operation

### *2.1 NRC Regulatory Position and Activities*

The existing NRC regulatory position effectively restricts remote operation: 10 CFR 50.54 requires licensed senior operators to be present at the facility, and RG 5.71 Rev.1 [6], which implements 10 CFR 73.54, prohibits remote access to Critical Digital Assets (CDAs) associated with safety related and important to safety functions as well as the use of wireless communication in safety systems. The NRC has also conducted stepwise regulatory preparatory activities for remote operation. The ground rules published in 2021 [1] define remote operation as the primary command and control of a plant from outside the site boundary. The cybersecurity related rules require, among others, dedicated and redundant communication channels and configuration management of security protocols. They also require physical security and cybersecurity inspections of both on-site and remote control rooms.

10 CFR Part 53 [2] took effect in April 2026. This performance based and technology inclusive framework introduces the cybersecurity requirements of 10 CFR 73.110. Its implementation guidance, RG 5.96 [3], departs from the uniform prohibition of remote access. Where remote access, control, or monitoring is needed, appropriate protection must be incorporated into the defensive architecture. In addition, it must be demonstrated that attack pathways leading to cyber-enabled accident scenarios (CEAS) or cyber-enabled intrusion scenarios (CEIS) are eliminated or adequately mitigated. RG 5.96 thereby establishes a performance based review basis for remote operation.

### *2.2 CNSC Regulatory Position*

The CNSC regulates cybersecurity through a framework linking regulatory documents and CSA standards to license conditions. CSA N290.7:21 [4] prohibits remote access to Cyber Essential Assets (CEAs) of high and moderate nuclear safety significance and requires that remote access to low significance CEAs be limited as far as practicable, with risk mitigation and documented assessment of residual risk. Thus, the remote control of safety functions is effectively not allowed, as in the U.S. However, the graded approach leaves room for limited remote access, provided that it can be justified through a documented risk assessment.

### *2.3 Industrial Standards and Research Trends*

Industrial standards remain restrictive toward remote access to safety systems: IEEE Std 7-4.3.2-2016 [7] prohibits all remote access to safety systems, and IEC 63096:2020 [8] prohibits the remote maintenance or control of instrumentation and control (I&C) systems through remote data connections from outside the plant. Meanwhile, the Idaho National Laboratory (INL) proposed a classification of remote operations into five

classes according to the level of remote access [9], as summarized in Table I. Class 1 permits only one way data transmission for remote monitoring; Class 2 permits predefined and validated whitelisted commands executed by on-site control programs; Class 3 permits the remote control of individual non-safety components; and Classes 4 and 5 extend remote control to safety significant and safety related systems, respectively.

INL assesses Class 1 as already deployed, Classes 2 and 3 as feasible, and Classes 4 and 5 as practically infeasible under the existing 10 CFR Parts 50 and 52 licensing framework (prior to Part 53). Classes 2 and 3 are considered acceptable only where the plant is designed such that reactor safety remains unaffected even if the remote infrastructure is fully compromised. This is achieved not by removing the inbound pathway, but by segmenting it from the safety systems in both function and network.

Table I: Remote operation classes proposed by INL [9]

| System | C1 | C2 | C3 | C4 | C5 |
|---|---|---|---|---|---|
| Non-safety systems | M | M | M&C | M&C | M&C |
| Safety significant and important to safety systems | M | M | M | M&C | M&C |
| Safety related systems | M | M | M | M | M&C |
| Feasibility | D | F | F | I | I |

C: class; M: monitoring; M&C: monitoring and control; D: deployed; F: feasible; I: infeasible (under the 10 CFR Parts 50/52 framework [9]).

### *2.4 Trends on Wireless Communication Security*

Wireless communication is highly considered as a communication means for remote control and monitoring. RG 5.71 Rev.1 [6] replaced the unconditional prohibition of wireless communication with concrete control requirements, permitting wireless access to CDAs only through boundary security control devices. Wireless use remains prohibited for CDAs associated with safety related and important to safety functions. In response to an industry request, the NRC stated that licensees must analyze, under 10 CFR 73.54(b)(1), whether wireless monitoring devices fall within the scope of their cybersecurity programs.

### *2.5 Regulatory Status in South Korea*

In South Korea, KINAC/RS-015 [5] provides the technical criteria for the cybersecurity of nuclear facilities. These criteria assume that critical systems operate within closed on-site networks. Accordingly, the security issues newly raised by remote operation, such as communication pathways outside the site, digital assets at remote facilities, and the authentication of remote operators, are areas that would require additional regulatory consideration. In addition, wireless connections to CDAs are prohibited in principle and allowed only exceptionally, after a vulnerability analysis and regulatory approval under RS-018 [10]. In short, while the U.S. has moved toward allowing wireless communication under security controls, South Korea maintains a more conservative approach based on prohibition in principle with case by case approval.

## 3. Conclusions

This paper examined domestic and international regulatory and standardization trends on cybersecurity for the remote operation of SMRs. While the NRC and the CNSC effectively restrict remote operation under their existing frameworks, the NRC has established a regulatory basis for remote operation through the performance based framework of 10 CFR Part 53 and RG 5.96, and the INL classification of remote operations and related industrial standards offer useful references for grading regulatory requirements. In Korea, additional regulatory considerations would be needed to accommodate remote operation. The trends analyzed in this study are expected to serve as a foundation for preparing cybersecurity regulations for the remote operation of Korean SMRs, including the i-SMR. As future work, formal attack trees and MITRE ATT&CK for ICS mappings tailored to SMR remote operation architectures will be developed to support the demonstration of attack pathway elimination or mitigation.

## ACKNOWLEDGMENTS

This work 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] U.S. Nuclear Regulatory Commission, Ground Rules for Regulatory Feasibility of Remote Operations of Nuclear Power Plants, USA, 2021.
[2] U.S. Nuclear Regulatory Commission, Risk-Informed, Technology-Inclusive Regulatory Framework for Commercial Nuclear Plants, Title 10, Code of Federal Regulations, Part 53, 2026.
[3] U.S. Nuclear Regulatory Commission, Establishing Cybersecurity Programs for Commercial Nuclear Plants Licensed under 10 CFR Part 53, Regulatory Guide 5.96, USA, 2026.
[4] CSA Group, Cyber Security for Nuclear Facilities, CSA N290.7:21, 2nd ed., 2021.
[5] Korea Institute of Nuclear Nonproliferation and Control, Regulatory Standard on Computer and Information System Security of Nuclear Facilities, KINAC/RS-015, South Korea.
[6] U.S. Nuclear Regulatory Commission, Cyber Security Programs for Nuclear Power Reactors, Regulatory Guide 5.71, Rev. 1, USA, Feb. 2023.
[7] Institute of Electrical and Electronics Engineers, IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations, IEEE Std 7-4.3.2-2016, 2016.
[8] International Electrotechnical Commission, Nuclear Power Plants—Instrumentation, Control and Electrical Power Systems—Security Controls, IEC 63096:2020, 1st ed., 2020.

[9] Idaho National Laboratory, Proposed Classifications of Remote Operations for Nuclear Reactors Based on Physical and Cybersecurity Considerations, USA, 2025.
[10] Korea Institute of Nuclear Nonproliferation and Control, Cyber Security of Wireless Connections in Nuclear Facilities, KINAC/RS-018, South Korea.