Transactions of the Korean Nuclear Society Autumn Meeting
Changwon, Korea, October 30-31, 2025

Regulatory Trends in Cybersecurity for Advanced Reactors Focusing on the Safety-Security Interface

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

***Keywords :** Safety-Security Interface, SSI, Cybersecurity, SMR

1. Introduction

The development of Small Modular Reactors (SMRs) and other advanced reactor concepts requires regulatory frameworks tailored to their distinct characteristics.

Well-structured regulatory guidance is critical not only for ensuring the safe and secure deployment of advanced reactors, but also for enabling effective responses to emerging risks associated with new technologies. Such a proactive approach ultimately supports both regulatory robustness and economic viability.

In this context, the International Atomic Energy Agency (IAEA) emphasized the need to integrate safety, security, and safeguards (3S) considerations from the design stage [1]. Since many advanced reactors are still in early development, this provides a unique opportunity to embed 3S principles directly into designs, facilitating a more coherent and proactive integration of the safety–security interface.

Cybersecurity has emerged as one of the most critical challenges for advanced reactors, as the extensive use of digital technologies introduces risks that were not sufficiently addressed in traditional nuclear regulation. Within the safety–security interface, considering cybersecurity is essential because cyberattacks on digital control or protection systems could simultaneously compromise safety functions and undermine physical security barriers. Moreover, as digital technologies continue to evolve rapidly, the importance of cybersecurity within nuclear regulation will only increase.

Against this background, this study reviews recent regulatory trends to evaluate how cybersecurity considerations are being incorporated into the evolving safety–security framework for advanced reactors.

2. Advances in NRC Cybersecurity Guidance

NRC's Regulatory Guide (RG) 5.96, titled "Establishing Cybersecurity Programs for Commercial Nuclear Plants Licensed Under 10 CFR Part 53", is currently issued in draft form as DG 5075. This draft provides structured guidance on establishing, implementing, and maintaining cybersecurity programs for commercial nuclear reactors licensed under 10 CFR Part 53—a framework specifically tailored for advanced reactor licensing. RG 5.96 is open for public comment and has not yet received final staff approval.

Compared with RG 5.71, "Cyber Security Programs for Nuclear Power Reactors", RG 5.96 shows a clear tendency toward a risk-informed, performance-based approach in anticipation of advanced reactor deployment [2][3]. Although it does not provide exhaustive, detailed instructions for every aspect of cybersecurity, it includes examples of quantitative risk assessment to illustrate how cyber risks can be evaluated and managed.

This suggests a shift from traditional operational controls and personnel-focused measures toward the proactive integration of cybersecurity considerations into reactor programs and design planning.

Table I: Comparison of NRC Regulatory Guides 5.71 and 5.96 (Draft) Category

	RG 5.71	Draft RG 5.96
Applicability	Commercial nuclear power plants licensed under 10 CFR Parts 50/52	Advanced reactors licensed under 10 CFR Part 53
Primary Objective	Establish and maintain a cyber security program to protect nuclear facilities	Provide a cyber security framework tailored to Part 53 advanced reactor licensing
Structure	Cyber security policy → Defensive measures → Program maintenance & audit	Governance framework → Risk-informed approach → Performance and quantitative assessment elements Regulatory

3. Introduction of Quantitative Assessment in RG 5.96

A notable innovation in Draft RG 5.96 is the presentation of a quantitative assessment example in Appendix B. This appendix is not intended as a prescriptive requirement, but rather to serve illustratively demonstration of how risk-informed methods could be applied in the cybersecurity domain. While licensees are not obligated to adopt this approach, its inclusion signals the NRC's recognition that future cybersecurity regulation may evolve toward more systematic and quantitative evaluation frameworks. In this sense, Appendix B can be interpreted less as an optional annex and more as a glimpse into the likely direction of regulatory thinking.

From an analytical perspective, this example can be understood as a deliberate attempt to bridge the

methodologies of cybersecurity and nuclear safety. Nuclear safety has a long tradition of applying Probabilistic Safety Assessment (PSA) techniques to quantify plant risks under various initiating events. The introduction of probabilistic reasoning into cybersecurity guidance suggests that future regulatory frameworks may aim to harmonize safety and security evaluations, leveraging existing PSA datasets where applicable.

Although RG 5.96 does not explicitly require the integration of PSA data, the structural similarity strongly implies such potential. Another important implication lies in methodological efficiency. By decoupling the initiating event from the downstream probabilistic evaluation of protective layers, the assessment approach described in Appendix B permits reusability of the latter calculations. In practice, this means that even when the initiating cyber event varies—whether through a network intrusion, insider manipulation, or supply chain compromise—the underlying defense-in-depth probability models can remain largely intact. This modularity could reduce analytical burden and improve cost-effectiveness in maintaining a cybersecurity risk assessment framework over the lifetime of a facility.

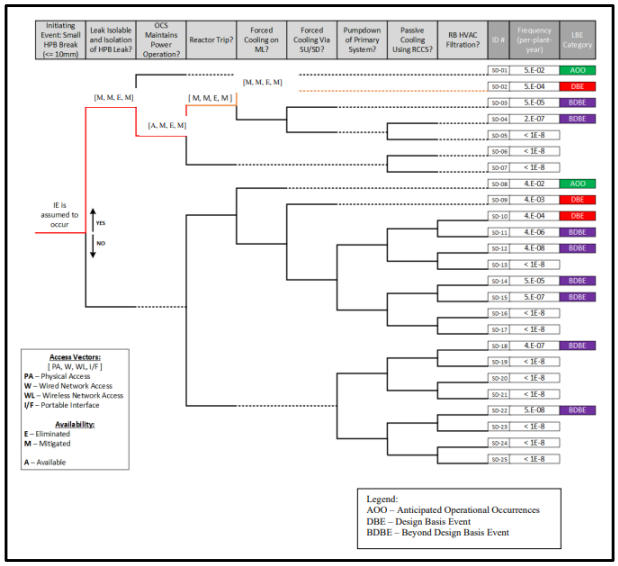

Fig. 1. Cyber-Enabled Accident Scenario: Illustrative Event Tree [2]

That said, the application of quantitative methods in cybersecurity also raises critical questions. Unlike equipment failure rates used in PSA, reliable statistical data on the likelihood of successful cyberattacks are scarce, context-dependent, and may evolve rapidly as adversary capabilities change. Thus, while RG 5.96 opens the door to a promising integration of risk-informed methodologies, its practical implementation will require careful calibration of assumptions, validation of data sources, and ongoing adaptation to the evolving threat landscape. In this sense, the quantitative example in Appendix B should be understood not as a prescriptive model, but as an initial conceptual step toward a more mature, data-driven cybersecurity regulatory framework.

4. Implications for the Safety–Security Interface

The regulatory shift represented by Draft RG 5.96 demonstrates how cybersecurity oversight is moving toward a risk-informed, performance-based paradigm. This evolution has direct implications for the safety–security interface (SSI), since cyber threats do not respect the traditional boundary between safety and security domains. A single digital intrusion can disable protective functions, distort operator response, and undermine physical barriers simultaneously.

By introducing probabilistic reasoning and structured assessment methods, RG 5.96 provides a mechanism to evaluate these cross-cutting vulnerabilities within a unified framework. In this way, cybersecurity regulation becomes more than a protective measure against digital risks—it serves as a conduit through which SSI can be operationalized in advanced reactor licensing and oversight.

5. International Regulatory Trends

Regulatory authorities in the nuclear sector worldwide are increasingly adapting their frameworks to support small modular reactors (SMRs) and other advanced technologies. While the level of specificity differs internationally, regulatory frameworks tend to emphasize risk-informed, performance-based, and technology-neutral approaches, reflecting the need for flexibility in licensing novel reactor designs where traditional prescriptive rules may be less effective.

Both the Canadian Nuclear Safety Commission (CNSC) and the UK's Office for Nuclear Regulation (ONR) stress efficiency and predictability in licensing. CNSC's SMR Readiness initiatives and ONR's refined Generic Design Assessment (GDA) and Security Assessment Principles (SyAPs) illustrate a focus on demonstrating safety and security outcomes rather than prescribing specific technologies.

Cybersecurity requirements remain less formalized than in the U.S., but regulators increasingly recognize the importance of the safety–security interface (SSI).

6. Summary and Implications

Attention to the safety–security interface (SSI) has grown within advanced reactor regulation, emphasizing the need to consider SSI from the earliest design stages. Within this context, cybersecurity has emerged as a critical factor that must be integrated alongside other safety and security measures. National and international frameworks are progressively shifting toward risk-informed, performance-based, and technology-neutral approaches, reflecting the unique characteristics of

small modular reactors (SMRs) and other novel designs. The NRC's Draft RG 5.96 illustrates how quantitative, risk-informed methodologies may be applied to cybersecurity programs, while regulatory initiatives in Canada (CNSC) and the UK (ONR) demonstrate parallel efforts to enhance efficiency, predictability, and performance-based regulatory evaluation.

Although formal cybersecurity requirements are less established in some countries, recognition of the SSI highlights the growing need to harmonize safety and security considerations. This trend suggests that future regulatory frameworks—including those under consideration in Korea—would benefit from proactive, integrated approaches that combine probabilistic assessment techniques with flexible, technology-neutral guidance. Ultimately, such measures can support both robust safety–security outcomes and the economic viability of advanced nuclear technologies.

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] IAEA, Time to Act: Integrating Safety, Security, and Safeguards in the Design of Innovative Reactor, "iaea.org/newscenter/news/time-to-act-integrating-safety-security-and-safeguards-in-the-design-of-innovative-reactors"
[2] U.S. Nuclear Regulatory Commission. (2024). DG-5075: Draft Regulatory Guide 5.96, Establishing Cybersecurity Programs for Commercial Nuclear Plants Licensed Under 10 CFR Part 53.
[3] U.S. Nuclear Regulatory Commission. (2023). Regulatory Guide 5.71, Revision 1, Cyber Security Programs for Nuclear Power Reactors.