Transactions of the Korean Nuclear Society Autumn Meeting
Gyeongju, Korea, October 29-30, 2026

Regulatory Trends in Cyber Security for Non-Light Water Reactors

Jae-Gu Song [a*], Ju Hyung Song [a]
[a]*Korea Atomic Energy Research Institute, Daejeon, South Korea*
[*]*Corresponding author: jgsong@kaeri.re.kr*

***Keywords :** non-light water reactor, cyber security, nuclear regulation, licensing, advanced reactor

1. Introduction

Development of non-light water reactors (non-LWRs), including sodium-cooled fast reactors (SFRs) and molten salt reactors (MSRs), has moved into actual licensing. These designs are being considered for a wider range of sites and operating conditions, such as marine and remote locations, and they make greater use of digital technology such as remote operation, autonomous operation and wireless communication. As a result, cyber security has become an item to be addressed from the design stage.

In Korea, work on SFRs, high temperature gas-cooled reactors (HTGRs) and MSRs is under way. In March 2026 an MSR-based nuclear-powered ship was selected as one of the twelve national missions of the K-Moonshot program, with the goal of starting construction by 2035. During that process, the need to prepare the licensing framework in advance, taking account of the characteristics of such ships, was raised [1]. The demand for a domestic licensing and regulatory framework for non-LWRs, including those for marine use, is therefore becoming concrete.

This paper reviews the cyber security regulatory frameworks of the U.S. Nuclear Regulatory Commission (NRC), the Canadian Nuclear Safety Commission (CNSC) and the U.K. Office for Nuclear Regulation (ONR), together with the licensing practice of major non-LWR vendors, using documents published by the regulators. The aim is to identify what is in place at present and where the regulations are heading.

2. Trends in Cyber Security Regulation for Non-LWRs

Of the three regulators, only the NRC has established a separate licensing pathway (10 CFR Part 53) and a separate cyber security rule (10 CFR 73.110) for advanced reactors (ARs), including non-LWRs [2,3]. Under the existing 10 CFR 73.54 (guidance in RG 5.71), assets are identified for protection according to whether they perform or support safety, security and emergency preparedness (SSEP) functions [4]. Under 73.110 (guidance in RG 5.96), the level of protection is graded according to the consequences a cyber attack could cause, which is a consequence-based approach [3,5]. The NRC has also issued a proposed rule for a separate licensing pathway for microreactors and reactors with comparable risk profiles (10 CFR Part 57), and the comment period is under way [6].

CNSC has not issued a separate cyber security technical standard for non-LWRs. It applies the existing design requirements (REGDOC-2.5.2) together with the cyber security standard CSA N290.7:21 [7]. At the same time, CNSC amended the Nuclear Security Regulations in November 2025 so that cyber security program requirements are set out at the level of the regulations, and extended their scope beyond high-security sites to other nuclear facilities. This followed a recommendation to introduce a risk-informed, graded approach for SMRs, and the supporting regulatory documents (the REGDOC-2.12 series) are being revised [8].

ONR has no provisions specific to a reactor type. It assesses designs against the Security Assessment Principles (SyAPs), which apply to all nuclear designs [9]. Rather than prescribing a list of controls and checking whether each has been implemented, SyAPs set out the security outcomes a dutyholder is expected to achieve and leave it to the dutyholder to demonstrate how they are met. Neither CNSC nor ONR distinguishes between light water and non-light water designs; for non-LWRs, the existing requirements are interpreted and applied to each design.

Taken together, all three regulators are moving toward graded, risk-informed protection, but they differ in whether this is done through new provisions or through existing ones.

3. Cyber Security Implementation by Non-LWR Vendors

Nine major vendors across five reactor types were reviewed, as of June 2026. Most are pursuing licensing with the NRC, and some are also using the CNSC Vendor Design Review (VDR) or the ONR Generic Design Assessment (GDA). Looking at the NRC applications, most vendors applied under the existing Part 50 or Part 52 before Part 53 came into force, so the cyber security rule that actually applies to them is still 73.54. No case has been found in which the consequence-based approach of 73.110 has been applied in an actual review. What follows therefore describes how vendors have addressed cyber security under 73.54.

For SFRs, TerraPower Natrium obtained a construction permit in March 2026, the first such permit for a non-LWR intended for commercial power generation; the earlier permits for Kairos Hermes and Natura MSRR were for a test reactor and a research reactor. At this stage the review goes only as far as

confirming that cyber security features are included in the design, and the detailed cyber security plan (CSP) will be submitted and reviewed with the operating license application.

For HTGRs, X-energy Xe-100 submitted a defensive computer security architecture (DCSA) that separates safety systems from non-safety systems and sets the boundary between them using one-way communication through devices such as data diodes. During the review, the NRC noted that the classification of safety-significant structures, systems and components (SSCs) and that of critical digital assets (CDAs) overlap considerably but are not the same, and asked that CDAs be identified and analyzed separately from a cyber security point of view [10]. Safety classification is thus a starting point for identifying assets to be protected, but it does not settle the matter on its own.

For MSRs, the joint NRC-CNSC review of the Terrestrial Integral Molten Salt Reactor (IMSR) raised the question of whether malicious acts such as cyber attacks should be included in the postulated initiating events (PIEs) used in the safety analysis. The regulators noted that malicious acts are normally addressed in a separate security assessment rather than in the safety analysis [11]. This matters for non-LWRs because passive and inherent safety features are often cited to argue that a cyber attack could not lead to serious consequences. Safety analysis, however, assumes random failures, while an attacker chooses what to disable and when. A separate security assessment is therefore still needed to decide how much protection a design requires.

It should also be noted that 10 CFR 73.54 applies, by its own terms, to licensees and applicants for an operating license for a nuclear power plant [4]. Facilities that are not intended for power generation, such as the Natura MSRR research reactor and the Kairos Hermes test reactor, therefore fall outside its scope.

4. Considerations for Non-LWR Cyber Security Regulation in Korea

The following points need to be considered in developing detailed criteria for cyber security regulation of non-LWRs in Korea.

First, the regulatory approach. Under NRC 10 CFR 73.54, which was written for existing power reactors, critical systems (CSs) and critical digital assets (CDAs) are identified according to whether digital assets perform SSEP functions or belong to support systems that could affect those functions, and cyber security controls are then applied to the assets so identified [4]. The new 73.110 was written because advanced reactors cover a wide range of designs, such as HTGRs, MSRs and liquid metal-cooled reactors, with different levels of risk depending on the technology used [12]. It identifies assets for protection according to whether a cyber attack could lead to an offsite radiological release or to compromise of physical security functions, and grades the level of protection according to the significance of that consequence. The accompanying guidance, RG 5.96, sets out a tiered analysis at the facility, function and system levels. CNSC and ONR, by contrast, have chosen to accommodate non-LWRs by interpreting and applying existing requirements and standards to each design rather than issuing separate criteria. Korea may wish to consider which of these routes is better suited to its own framework whether to follow the NRC approach of preparing a separate technical standard for non-LWRs, or the CNSC and ONR approach of extending and interpreting the existing standard (KINAC/RS-015 [13]).

Second, the scope of application and what to review at each licensing stage. It would be useful to set criteria according to the purpose of the facility, whether power generation, research or demonstration, and the type of license, and it should be clear what is to be confirmed at each stage, that is, standard design approval, construction permit and operating license. This is also related to the recent amendment of the Act on Physical Protection and Radiological Emergency, which introduced submission and approval requirements at the standard design approval stage. Non-LWRs are likely to begin as research-type facilities and then move to a standard design, so at the early stage, when the design is not yet fixed, one option would be to look first at matters that are hard to change later, such as the defensive architecture (DCSA) and the setting of communication boundaries, from a security by design perspective, and to let detailed controls and operating procedures be developed step by step during construction and operation. Such a flexible approach could reduce the burden of design change on the vendor and the burden of review on the regulator.

Third, the regulatory direction for new technologies and how it might be applied in Korea. Remote and autonomous operation, wireless communication and supply chain security are areas where requirements have not been settled even abroad, so it would be helpful to follow international developments and prepare the domestic direction in advance. Because design characteristics and risk levels differ from one reactor type to another, a single set of criteria may not be suitable for all designs; further work on how a risk-informed, technology-neutral approach can be applied to cyber security would therefore be useful. In addition, as remote operation and unmanned operation reduce the number of staff on site and the physical controls that go with them, the line between physical security and cyber security becomes less clear, so measures against blended attacks that combine physical intrusion with cyber attack may need to be considered. For non-LWRs, where passive and inherent safety characteristics bear directly on how the consequences of a cyber attack are assessed, design and regulatory approaches that take the safety-security interface (SSI) into account need to be developed.

5. Conclusions

This paper has reviewed the cyber security regulatory frameworks of the NRC, CNSC and ONR and the licensing practice of major non-LWR vendors. Regulation abroad is moving toward a risk-informed, consequence-based and graded approach, but it is still taking shape and applied cases have yet to accumulate. The way the frameworks are being developed also differs: the NRC has issued new provisions for advanced reactors, while CNSC and ONR make use of their existing technical standards. On this basis, three points have been suggested for cyber security regulation of non-LWRs in Korea: the regulatory approach, the scope of application together with what to review at each licensing stage, and the regulatory direction for new technologies and its application in Korea. The results are expected to serve as a basis for future work on a domestic cyber security regulatory framework for non-LWRs.

Acknowledgements

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-2025-02313625)

REFERENCES

[1] Ministry of Science and ICT, Press releases on the K-Moonshot SMR Ship Mission industry meeting (30 April 2026) and the launch of the K-Moonshot Project (28 May 2026).

[2] U.S. NRC, Risk-Informed, Technology-Inclusive Regulatory Framework for Advanced Reactors (10 CFR Part 53), 91 FR 15794, 2026.

[3] U.S. NRC, 10 CFR 73.110, Technology-inclusive requirements for protection of digital computer and communication systems and networks.

[4] U.S. NRC, 10 CFR 73.54, Protection of digital computer and communication systems and networks.

[5] U.S. NRC, Establishing Cybersecurity Programs for Commercial Nuclear Plants Licensed under 10 CFR Part 53, RG 5.96, 2026.

[6] U.S. NRC, Licensing Requirements for Microreactors and Other Reactors With Comparable Risk Profiles (Proposed Rule, 10 CFR Part 57), 91 FR 23628, 2026.

[7] CSA Group, Cyber Security for Nuclear Facilities, CSA N290.7:21, 2021.

[8] Canada, Nuclear Security Regulations, SOR/2025-219, 2025.

[9] ONR, Security Assessment Principles for the Civil Nuclear Industry, 2022.

[10] U.S. NRC, Audit Report of X-energy Xe-100 PCDAS White Paper, ML23236A008, 2023.

[11] U.S. NRC and CNSC, Joint Report on Terrestrial Energy's Methodology for Developing a Postulated Initiating Events List for the IMSR, ML22139A124, 2022.

[12] I. Garcia, J. Jauntirans and M. Rowland, U.S.A. Regulatory Efforts for Cyber Security of Advanced Reactors, IAEA-CN-308, ML22284A126, 2022.

[13] KINAC, Computer and Information System Security at Nuclear Facilities, KINAC/RS-015 Rev.02, 2023.