Analysis of regulatory trends for cyber security in SMRs

Jae-Gu Song [a*], Kwang-Seop Son [a], Cheol Kwon Lee [a], Jung Woon Lee [a], Young-Jun Lee [a]
[a]*Korea Atomic Energy Research Institute, 111, Daedeok-daero 989 beon-gil, Yuseong-gu, Daejeon, 34057*
[*]*Corresponding author: jgsong@kaeri.re.kr*

***Keywords :** framework for regulation, technology for nuclear security for SMR, cyber security for SMR, security by design

1. Introduction

Small Modular Reactors (SMRs), currently under development worldwide, are expected to have different design characteristics, giving rise to novel licensing considerations not found in traditional large nuclear power plants [1, 2]. This paper identifies common cyber security concerns relevant to SMRs, arising from the technologies and design characteristics envisaged for emerging applications. It also describes the direction of the cyber security regulatory frameworks of the U.S. Nuclear Regulatory Commission(NRC), Canadian Nuclear Safety Commission(CNSC) and the UK Office for Nuclear Regulation(ONR), which are leading the way in the regulation of SMRs.

2. SMR Cyber security Technology Development Trends

2.1 Emerging Technologies that Require Cyber Security Considerations

According to the IAEA's ongoing "Instrumentation & Control and Computer Security for SMRs/MRs" Consultancy Meeting (CM) and Technical Meeting (TM) [3], the followings are being considered as key technical issues to add to the existing nuclear cyber security considerations.

- New Digital Technologies
- Remote Operations
- Autonomous Operations
- Regulatory Approaches
- Safety Security Integration
- Supply Chain Security

2.2 Cyber Security Implementation Status of Major Developers

2.2.1 NuScale

NuScale has submitted a cyber security programme to comply with the NRC regulations regarding the cyber security methodology and the approach to implementing the CSP for the US600 and US400 models under development [4]. Key details of the programme are as follows:

- Security by Design: This involves the application of cyber security policies during the design and procurement processes, including cyber security requirements in software development processes such as Secure Development and Operation Environment (SDOE). In addition, it specifies the inclusion of cyber security requirements in the design specifications of all digital components (devices) as part of the standard design.
- Defensive Architecture: It specifies the design of a layered system structure in which communication between business systems and the security and control systems is restricted, thereby ensuring security.
- Defense-in-Depth: Implementation of defence-in-depth measures
- Supply Chain: Consideration of a risk management programme to monitor the supply chain.

2.2.2 Rolls-Roys

Rolls-Royce(RR) has recently announced the completion of Phase 1 Generic Design Assessment (GDA) for the Generic RR SMR. As part of this process, a Preliminary Security Report (PSyR) has been developed, which is expected to serve as the foundation for the forthcoming Generic Security Report (GSR) and other related documents [5]. The main points (claims) of the GSR are as follows:

- Security by Design
- Protection from Sabotage
- Protection from Theft
- Cyber Security & Information Assurance

3. Regulatory Trends for Cyber Security in SMRs

3.1 U.S. NRC

Regulations related to nuclear power plant construction, design certification, and standard design approval by the U.S. NRC have been conducted through evaluations under the statutes of 10CFR50 and 10CFR52. Nuclear security (physical security and cybersecurity) has been regulated based on the provisions of 10CFR73 [6]. Among these, cyber security is primarily grounded in 10CFR73.1 and 10CFR73.54.

The NRC is in the process of developing regulatory guidelines to implement the advanced reactor cyber security regulation, 10CFR73.110, "Technology neutral requirements for protection of digital computer and communication systems and networks". These guidelines are being developed with the support of cyber security experts [7]. Given that 10CFR73.110 is expected to serve as the basis for future SMR cyber security regulations, the regulatory requirements outlined in this statute are perceived as essential documents that U.S. SMR developers must definitely take into account.

3.2 Canada CNSC

Canada, actively engaged in SMR development, has implemented the Vendor Design Review (VDR) process [8] from the early stages of development, with regulatory authorities participating to review anticipated licensing issues from a regulatory perspective, aiming to alleviate the developer's burden. REGDOC-2.5.2 (Design of Reactor Facilities: Nuclear Power Plants, CNSC, 2014) [9] provides requirements and guidance for new licence applications for nuclear reactor facilities. This document outlines comprehensive design requirements and guidelines that are consistent with international regulations and practices based on risk information.

Specifically, section 7.22.4 of REGDOC-2.5.2 provides detailed regulatory guidance concerning the cyber security design of nuclear reactor facilities, along with the following overarching regulatory requirements:

-The design of computer-based I&C systems important to safety shall provide a cyber security defensive architecture.

-Computer-based I&C systems and components important to safety shall be protected from cyber attacks in order to maintain confidentiality, integrity and availability.

-A cyber security program shall be developed, implemented and maintained so as to achieve the security required in each phase of the computer-based I&C systems' lifecycle.

-Cyber security features shall not adversely affect the functions or performance of SSCs important to safety.

3.3 UK ONR

In the United Kingdom, there are key laws related to nuclear security regulation, namely the Nuclear Installation Act (1965) [10] and the Nuclear Industry Security Regulation (2003) [11]. ONR, in collaboration with the Environment Agency and Natural Resources Wales (NRW), has introduced the Generic Design Assessment (GDA) process [12]. This process evaluates whether nuclear construction and operation meet regulations pertaining to safety, security, environmental protection, and waste management.

The Generic Design Assessment (GDA) facilitates regulatory involvement in the early stages of design, enabling applicants to assess or address licensing issues early on [13]. The Office for Nuclear Regulation (ONR) specifies that they evaluate security-related documents (Generic Security Report), such as security plans, security measures, and cyber risk assessments, submitted by applicants, according to Security Assessment Principles (SyAP) and Fundamental Security Principles (FSyP). Key regulation aspects include the following:

- Secure by design
- Graded approach
- Defense-in-depth
- Security categorization
- Security classification
- Codes and standards

3. Conclusions

This study analyses the status of the application of cyber security technology in overseas small modular reactors (SMRs). The cyber security related legislation and regulatory guidelines of the United States, Canada and the United Kingdom, which are leading in SMR regulation, are explained.

For the export-oriented i-SMR, considering the regulatory framework of foreign licensing authorities described in this study, there is a need to establish a cyber security regulatory process early on and incorporate it into the design phase with designer and regulator. These efforts must be part of the domestic pre-licensing process and design, but are also essential for potential exports.

Acknowledgements

This work was supported by the Nuclear Safety Research Program through the Korea Foundation Of Nuclear Safety (KoFONS), granted financial resource from the Nuclear Safety and Security Commission (NSSC), Republic of Korea. (No. 2202022)

REFERENCES

[1] IAEA, Advances in Small Modular Reactor Technology Developments 2020 Edition : A Supplement to IAEA Advanced Reactors Information System(ARIS), 2020.

[2] IAEA, Lessons Learned in Regulating Small Modular Reactors-Challenges, Resolutions and Insights, IAEA-TECDOC-2003, 2022.

[3] Busquim Rodney, Instrumentation & Control and Computer Security for SMR/MRs, Technical Meeting on the Status, Design Features, IAEA Technology Challenges and Deployment Models of Microreactors, 2021.

[4] NuScale Power, Carbon Free Power Project (CFPP) Combined License Application (COLA) Presentation, Cyber Security Program (Open Session), PM-134195-NP, Revision 0, 2023.

[5] Rolls-Royce, Rolls-Royce Small Modular Reactor (RR SMR) - Preliminary Security Report (PSyR), Rolls-Royce SMR Ltd, TS-DD-01 Issue 3, SMR0001610 Issue 1, 2023.
[6] Jacopo Buongiorno, Michael Corradini, John Parsons, David Petti, et al., The Future of Nuclear Energy in a Carbon-Constrained World, Massachusetts Institute of Technology Energy Initiatvie, 2018.
[7] Ismael Garcia, Juris Jauntirans, Michael Rowland, Risk Informed, Technology-Inclusive Regulatory Framework for Advanced Reactors, IAEA International Conference on Topical Issues in Nuclear Installation Safety: Strengthening Safety of Evolutionary and Innovative Reactor Designs, 2022.
[8] CNSC, Pre-Licensing Vendor Design Review, http://nuclearsafety.gc.ca/eng/reactors/power-plants/pre-licensing-vendor-design-review/index.cfm (accessed August 16, 2023)
[9] CNSC, REGDOC-3.5.3, Regulatory Fundamentals, https://nuclearsafety.gc.ca/eng/acts-and-regulations/regulatory-documents/published/html/regdoc3-5-3/index.cfm (accessed August 16, 2023)
[10] ONR, Nuclear Installations Act 1965, https://www.legislation.gov.uk/ukpga/1965/57 (accessed August 16, 2023)
[11] ONR, The Nuclear Industries Security Regulations 2003, https://www.legislation.gov.uk/uksi/2003/403/contents/made (accessed August 16, 2023)
[12] ONR, NRW, Use of UK Climate Projections 2018 (UKCP18) Revision 2, 2022.
[13] ONR, New Nuclear Power Plants: Generic Design Assessment Technical Guidance, ONR-GDA-GD-007 Revision 0, 2019.