# STUDY ON Standard design review area

# for cyber security-by-design of Smr

KOOKHEUI KWON

Korea Institute of Nuclear Nonproliferation and Control

Daejeon, Republic of Korea

Email: vivacita@kinac.re.kr

SUBONG LEE

Korea Institute of Nuclear Nonproliferation and Control

Daejeon, Republic of Korea

Email: sblee@kinac.re.kr

HYUNJOO LEE

Korea Institute of Nuclear Nonproliferation and Control

Daejeon, Republic of Korea

Email: sn220865@kinac.re.kr

**Abstract**

Compared to large nuclear power plants, SMRs have many novel aspects and limitations, which may affect not only safety but also security. Therefore, it is essential to design SMR holistically, by integrating cyber security, into an effective system. As cyber threats evolve rapidly, and the use of programmable digital systems increases, integrated design of cyber security, is important to achieve robustness of the SMR's security system. For these reasons, this paper will analyze cyber security areas that need to be reviewed from security perspective for various standard design of SMRs, and covers key references for review, interface with other technical areas, documents required from venders, review criteria to consider.

## INTRODUCTION

Nuclear energy has emerged as a crucial power source globally, constituting approximately 10% of the total energy sources. In the Republic of Korea, as of 2022, nuclear energy accounts for 29.6% of the total electricity generation. However, there is a growing need to enhance nuclear safety post the Fukushima disaster and to consider improvements in nuclear energy utilization, such as accommodating the increasing coexistence of renewable energy sources. Therefore, attention has turned to Small Modular Reactors (SMRs) technology.

To ensure the safe utilization of nuclear energy, regulatory measures for cyber security concerning of digital assets of nuclear facilities are being enforced. As part of these regulations, new nuclear facilities undergo on review of their cyber security plan and implementation results to ensure compliance. However, due to differences in design features between SMRs and existing nuclear power plants, such as system simplification, wireless communication, smart sensors, there is a need to assess the applicability of existing review guidance.

Nuclear security measures are required for nuclear power plants to prevent radiological sabotage and unauthorized removal of nuclear materials, and for this purpose, prevention, detection, and response security measures for physical protection and cyber security are performed and related systems are installed.

As these cyber security measures and systems are related to the plant design and can affect plant safety and operations, the IAEA Nuclear Security Series and Safety Standards require integrated consideration from the plant design stage, as followings;

* IAEA Nuclear Security Series No. 13 (INFCIRC/225/Rev. 5, 2011), “Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities”

(Fundamental Principle E : Responsibility of License Holders) For a new nuclear facility, the site selection and design should take physical protection into account as early as possible and also address the interface between physical protection, safety and nuclear material accountancy and control to avoid any conflicts and to ensure that all three elements support each other.

* IAEA Safety Standards No. SSR-2/1 (Rev.1, 2016), “Specific Safety Requirements of Nuclear Power Plants: Design”

(Requirement 8 : Interface of safety with security and safeguards) Safety measures, nuclear security measures and arrangements for the State system of accounting for, and control of, nuclear material for a nuclear power plant shall be designed and implemented in an integrated manner so that they do not compromise one another.



*FIG. 1. General Cyber security-by-design activities during development*

In particular, compared to large nuclear power plants, SMRs have many novel aspects and limitations, which may affect not only safety but also security. Novel risks affecting SMR cyber security include the following, which should be integrated and mitigated in the design engineering process of SMRs.

* A variety of wired & wireless communications and digital technologies, autonomous operations, and remote monitoring may increase cyber risk
* Potentially different security risks because of the SMRs' compact designs and connections. If all targets and safety features are connected in a small area and can be destroyed at the same time, the added value of nuclear security for safety features will be significantly reduced
* Multiple unit sites increase the nuclear inventory and thereby the security risk, but shared services may have positive implications for both safety and security
* Remote sites and mobile units may present challenges for adequate and timely off-site response
* Modularization and standardization may increase supply chain risk

Therefore, it is essential to design SMR holistically, by integrating cyber security into an effective system. As cyber threats evolve rapidly, and the use of programmable digital systems increases, integrated design of cyber security is important to achieve robustness of the SMR's security system.

For these reasons, this paper will analyse cyber security areas that need to be reviewed from security perspective for various standard design of SMRs, and covers review strategy, key references for review, standard review area, review criteria to consider.

## Standard design review for cyber security-by-design

### Review Strategy

The basic goal is to examine whether the operator establishes the cyber security program appropriately, including design, manufacturing, installation, and procedure development in consideration of security requirements from the design stage to systematically operate the cybersecurity program of the operating nuclear facility. To this end, the review direction of the standard design approval stage is as follows.

* Validity of the conceptual design of the standard design stage
* Adequacy of the design basis, including methodology, principles, and procedures to meet regulatory requirements
* Functional and performance requirements for intended security and adequacy of design basis for detailed design
* Security considerations of the selected major digital platforms (results of security measures applied according to the security assessment, etc.)

### Key References for Review

* IAEA Safety Standards, Specific Safety Requirements No. SSR-2/1 (Rev. 1) “Safety of Nuclear Power Plants: Design” - Requirement 8, Interfaces of safety with security and safeguards
* No. 42-G, Implementing Guide, “Computer Security for Nuclear Security”
* No. 17-T (Rev. 1), Technical Guidance, “Computer Security Techniques for Nuclear Facilities”
* No. 33-T, Technical Guidance, “Computer Security of Instrumentation and Control Systems at Nuclear Facilities”

The IEC standard series “IEC 62645, Nuclear power plants – Instrumentation, control and electrical power systems – Cybersecurity requirements” and “IEC 62859, Nuclear power plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity” also provide additional benchmark requirements.

### Standard Design Review Area

The vendor should provide information to justify that cyber security have been considered in the SMR standard design and integrated engineering process for it. To facilitate standard design review by regulators, vendors should provide the following information;

* General Design process and requirements for Cyber Security
* Sensitive Digital Systems/Assets Identification & Classification
* Design information for Defensive Cyber Security Architecture (Security Level and Segmentation, Communication control between levels, etc)
* Cyber security assessment and Security-by-Design Information for cyber risk mitigation of Sensitive Digital Systems/Assets
* Cyber event monitoring/detection system
* Security Strategy for cyber supply chain risk

TABLE 1. Standard Design Review Area for Cyber Security

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Plan Review | Security Team | Target Analysis | Security Architecture | Security Assessment | Security Measure | Response Measure |
| Design Review Area | Adequacy of security design plans to meet regulatory requirements within standard designs | Feasibility of organizational activities and approaches for Security by Design (SeD) consideration of security requirements in the standard design phase | - Appropriateness of Security Subject Identification Methodology/Procedures (Essential Systems/Essential Digital Assets)  - Appropriateness of the result(s) of identification of essential systems according to the standard design | - Validity of cybersecurity defensive architecture (CS Defensive Architecture) approach, including security classification and compartmentalization within the essential system  - Security classification according to standard design, validity of defensive structure design results (including wired and wireless communication)  - Validity of N/W security facility functions/performance requirements within the defense structure | - Appropriateness of security assessment methodology/procedures  - Validity of security assessment results (standards) for selected secure and unsecure digital platforms (PLC, DCS, FPGA, etc.) | - Appropriateness of security measures methodology/procedures based on security assessment results (standard)  - Appropriateness of security measures results/implementation based on security assessment results for selected secure/unsecure key digital platforms (PLC, DCS, FPGA, etc.) (Standard) | - Adequacy of methodology for cybersecurity monitoring (detection, alarms, logs)  - Adequacy of facility/equipment capabilities/performance requirements for cybersecurity monitoring (detection, alarms, logs) |

### Review Criteria for Cyber Security

IAEA Safety The regulators could consider the following nuclear security criteria as part of their pre-licensing review.

#### General Design process and requirements for Cyber Security (NSS 17-T 6.11-6.20)

1. The operator should use the output of the facility CSRM work conducted during the planning stage to ensure that the facility design process provides for computer security requirements for facility functions (expressed in the DCSA and the CSP) to be met as an integral part of the system engineering activities for the facility. This applies to the design of a new facility or to the modification of the design for refurbishment or modification of the facility during the operation stage of the facility.
2. The design process should take into account computer security requirements that arise owing to the dependencies between facility functions, as identified during the facility CSRM process.
3. Computer security requirements should be provided in sufficient detail to allow design decisions to be made, the design to be verified and design changes to be evaluated.
4. The operator should perform system CSRM for each system, including verification at each step of the design of the computer security measures.
5. Physical and remote accessibility of the SDAs within vital areas by an insider should be considered at the design stage.
6. The operator should develop computer security validation criteria for the commissioning stage. Systems performing facility functions assigned the highest computer security levels should be independently validated.

#### Identification of Sensitive Digital Assets (NSS 42-G 2.10-2.20)

1. Owners and/or designers of computer based systems should use a systematic process to identify the functions performed by their digital assets that are required for nuclear security and safety, any associated SDAs, and the potential effect on nuclear security and safety if any SDAs are compromised. In doing so, they should recognize that a computer based system that does not itself contain SDAs could nevertheless, if compromised or infected with malware2, potentially affect SDAs in other systems.
2. The first step in a systematic process should be to identify the functions that directly support one or more aspects of nuclear security (e.g. physical protection, nuclear material accounting and control and sensitive information management) and nuclear safety. The computer based systems and component digital assets that support those functions should then be identified.

#### Defensive Cyber Security Architecture (NSS 17-T 4.67-4.70)

1. The operator should design and implement a DCSA in which all systems performing facility functions are assigned to a computer security level and protected according to computer security requirements specified for that level.
2. The operator should specify those baseline computer security measures that are mandatory for each computer security level within the DCSA. These baseline measures may include technical, administrative and physical control measures.
3. The DCSA should be designed to eliminate or limit the possible routes for cyber‑attack (as identified in the threat characterization) that an adversary could exploit to compromise systems performing facility functions. Similar processes for reducing physical pathways available to the adversary are detailed.
4. Computer security boundaries should be established between systems performing facility functions that have different computer security levels.

#### Cyber Security Assessments (NSS 33-T 4.95-4.100)

1. The guidance provided in paras 4.96–4.100 applies to all I&C systems, subsystems and components having an assigned security level.
2. Computer security assessments should be performed for each phase of the I&C system life cycle to identify potential threats as well as vulnerabilities and weaknesses.
3. Public or open source information as well as vendor, contractor or supplier and expert sources should be monitored to promptly identify changes in the threat landscape and new vulnerabilities.
4. New or changed threats and vulnerabilities should be assessed to evaluate their potential impact on I&C system computer security. Corrective action (e.g. amended security features) should be taken if these changes could result in potential security violations or unacceptable risks for the facility.
5. Each organization that is responsible for developing, deploying, operating, maintaining or decommissioning I&C systems or components should perform periodic computer security assessments and audits.
6. The results of the computer security assessments should be used to update the system CSRM

## Conclusion and future plan

This study analyzed the cyber security areas that require review in the standard design of Small Modular Reactors (SMRs). Integrating cyber security into the SMR design process from the earliest stages is essential to address the unique risks and limitations of SMRs compared to larger nuclear power plants.

The compact and interconnected nature of SMRs, along with their use of various digital technologies and autonomous operations, introduces novel cyber security risks. These include potential vulnerabilities due to the proximity of critical systems, the challenges of remote and mobile units, and increased supply chain risks. Therefore, a comprehensive and integrated approach to cyber security is necessary to ensure the robustness of SMR security systems.

Our analysis identified critical areas for standard design review, such as the validity of security design plans, the adequacy of security assessments, and the implementation of defensive cyber security architecture. These areas are aligned with the guidelines and standards set by the International Atomic Energy Agency (IAEA) and other relevant regulatory bodies.

Future study will focus on developing specific evaluation methods and criteria for cyber security in SMR designs. This includes creating detailed procedures for cyber security assessments and validation. Additionally, conducting case studies on the implementation of cyber security measures in existing and new SMR projects will provide valuable insights into best practices and areas for improvement. Further studies should also explore the integration of cyber security with other safety and security measures to ensure a comprehensive approach that does not compromise any aspect of SMR operations.

ACKNOWLEDGEMENTS

This work was supported by the Korea Foundation of Nuclear Safety (KoFONS) grant funded by the ROK government Nuclear Safety and Security Commission (NSSC) (2207008-0122-CG100).

References

1. Safety Regulatory Direction Guide for SMRs, Nuclear Safety and Security Commission, 2023
2. Kookheui K., Analysis of Nuclear Security Review Cases for the NuScale Standard Design Approval, KINAC/TR-011/2022(C2-9320), Korea Institute of Nuclear Nonproliferation And Control, 2022.
3. KINAC/RS-015, “Cyber Security Regulatory Standard for Nuclear Facilities”, KINAC, 2014.
4. Nuclear Security Series No.17. “Computer Security at Nuclear Facilities”, IAEA, 2011
5. Nuclear Security Technical Guide No.36. “Computer Security of Instrumentation and Control Systems at Nuclear Facilities”, IAEA, 2017
6. International Physical Protection Advisory Service. “IPPAS Mission Report for the Republic of Korea”, IAEA, 2014
7. Draft Nuclear Energy Series. “Engineering and Design Aspects of Computer Security for Instrumentation and Control Systems at Nuclear Power Plants”, IAEA, 2017
8. IEC 62645. “Nuclear Power Plants – Instrumentation and Control Systems – Requirements for Security Programmes for Computer – based Systems”, IEC, 2014
9. DICWG-08. “Common Position on the impact of Cyber Security Features on Digital I&C Safety Systems”, OECD NEA, 2012
10. Vitor M. McCree, Executive Director for Operations. “Security Considerations in New Reactor Construction”, U.S. NRC, 2016
11. Security Guide for Software Development, “Software development security guide for e-government software developers”, KISA, 2017
12. Regulatory Guide 5.71. “Cyber Security Program for Nuclear Facilities”, U.S. NRC, 2010
13. Nuclear Energy Series(draft). “Engineering and Design Aspects of Computer Security for I&C systems at Nuclear Power Plants”, IAEA, 2017
14. IAEA Safety Standards No. SSG-39. “Design of Instrumentation and Control Systems for Nuclear Power Plants”, IAEA, 2016
15. NEI 13-10(rev.6). “Cyber Security Control Assessments”, NEI, 2017
16. NIST Planning Report 02-3. “The Economic Impacts of Inadequate Infrastructure for Software Testing”, NIST, 2002
17. NIST 800-53(rev.2). “Guide to Industrial Control System Security”, NIST, 2015