A Study on Security Verification and Validation (V&V) Regulatory Trends for Small Modular Reactors

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

Keywords : Verification and Validation, Small Modular Reactors, Cybersecurity, Secure Development and Operational Environment

1. Introduction

With the global expansion of Small Modular Reactors (SMRs), ensuring security has emerged as a critical concern, particularly in light of emerging technologies such as wireless-based remote control and AI-driven autonomous operation. To this end, it is essential to derive security requirements, implement appropriate countermeasures, and evaluate their effectiveness throughout the SMR lifecycle. In this context, it is imperative that Verification and Validation (V&V) serve as a critical mechanism for assessing whether those security requirements are properly defined, effectively implemented, and consistently maintained in compliance with regulatory and industrial standards.

The International Atomic Energy Agency (IAEA) has underlined the necessity of V&V for security requirements throughout the SMR lifecycle through a series of technical guides [1-3]. In particular, IAEA NSS 33-T [1] emphasizes V&V activities for security requirements applied to all I&C systems, subsystems, and components assigned security levels in nuclear facilities. In South Korea, recent initiatives have been launched to establish legal and regulatory foundations for enforcing cybersecurity requirements from the design phase of nuclear facilities. Nevertheless, a comprehensive regulatory framework and systematic methodology for security V&V in SMRs remain underdeveloped.

Against this backdrop, this study analyzes the regulatory and standardization trends concerning V&V from a security perspective, with the aim of deriving key insights and considerations to ensuring security of SMRs. To this end, the regulatory position of the U.S. Nuclear Regulatory Commission (NRC) on security V&V is reviewed in this paper. In addition, industrial standards such as those developed by IEEE and IEC are analyzed to identify guidelines for security V&V. Finally, based on the analysis of regulatory and industrial standardization trends, this study derives considerations and insights for security V&V, which are expected to contribute to the development of a regulatory framework for Korean SMRs.

2. Regulatory and Standardization Trends on Security V&V

In this section, regulatory position of the NRC regarding security V&V in nuclear facilities is examined as a crucial reference. In parallel, relevant guidelines provided by international industrial standards(IEEE, IEC) for security V&V are investigated to derive well-defined insights and considerations for establishing a comprehensive security V&V regulatory framework.

2.1 NRC Regulatory Position

The NRC is the primary regulatory authority in the U.S. for nuclear facilities. To examine its stance on security V&V, the following regulatory guidance documents were analyzed: RG 5.71 Rev.1 [4], RG 1.168 Rev.2 [5], and RG 1.152 Rev.4 [6]. Among them, RG 5.71 [4] provides guidance for establishing, implementing, and verifying cybersecurity programs for digital systems in nuclear power plants. While this guidance emphasizes the necessity of performing verification for security requirements, it does not provide concrete methodologies or detailed procedures for conducting such activities.

RG 1.168 Rev.4 [5] offers methodologies for performing verification, validation, technical and management reviews, and audits on digital computer software used in the safety systems of nuclear power plants. While this guidance endorses IEEE Std. 1012-2004 [7], it limits the scope of the security analysis V&V described in the standard to accidental or non-malicious events. That is, the Secure Development and Operational. Environment (SDOE) for unintentional acts is addressed within this regulatory guide, whereas deliberate malicious attacks are governed under RG 5.71.

RG 1.152 Rev.4 [6] provides guidance for ensuring high functional reliability, design quality, and adequate SDOE for programmable digital devices (PDDs) used in the safety systems of nuclear power plants. This guidance, which endorses IEEE Std. 7-4.3.2-2016 [8], presents specific instructions for establishing an SDOE lifecycle approach by endorsing Annex D of the standard.

Based on the overall review of these documents, the NRC regulatory position on security V&V can be summarized as follows:

- Security requirements for nuclear facilities are required to be verified.

- A SDOE-based V&V approach is established to address accidental or non-malicious events during the development of digital safety systems.
- Security analysis aimed at mitigating intentional or malicious acts for safety systems is not explicitly included within NRC V&V activities.

2.2 IEEE Standards

A series of IEEE standards relevant to security V&V have been published, including IEEE Std. 7-4.3.2-2016 [8] and IEEE Std. 1012 (2004 [7], 2012 [9], 2016 [10]). Earlier editions of IEEE Std. 7-4.3.2, such as the 2003 version, did not address the SDOE. Starting from the 2016 edition, SDOE is explicitly incorporated.

IEEE Std. 7-4.3.2-2016 [8] defines SDOE as a structural requirement to ensure the security of digital safety systems throughout their development and operational environments. The standard adopts a lifecycle approach to SDOE, specifying evaluation and management activities from the concept phase through verification, implementation, and installation. Key requirements for each phase are summarized as follows:

- Concept phase: Identify security requirements and potential vulnerabilities at the initial system design stage.
- Requirement phase: Precisely define SDOE requirements.
- Design phase: Translate SDOE requirements derived from system requirements into detailed design elements.
- Implementation phase: Ensure consistency and accuracy during software implementation. Assess whether new vulnerabilities are introduced during coding and consider the use of Commercial Off-The-Shelf (COTS) components.
- Test phase: Include controls and mitigation measures to maintain SDOE in the actual operational environment.
- Installation and checkout phase: Implement controls and mitigation measures to maintain SDOE in the actual operational environment.
- Operation and maintenance phase: Maintain a secure operational environment, following strict change management procedures for any modifications.
- Retirement phase: Define and implement measures to protect sensitive security information during system decommissioning.

IEEE 1012-2004 [7] provides criteria for assessing whether software fulfills its requirements and meets its intended purpose and user needs through a V&V process. The V&V process is applied throughout the entire software development lifecycle, with procedures specified according to the designated software integrity level. This standard specifies V&V tasks, inputs, and outputs for security analysis corresponding to each phase of the V&V process. However, the NRC restricts the application of this security analysis V&V to accidental or non-malicious events.

IEEE Std. 1012-2012 [9] and 2016 [10] expand the V&V processes to cover system, hardware, and software components. These standards introduce descriptions of security analysis that were not covered in IEEE Std. 1012-2004, provided in the annexes. In particular, IEEE Std. 1012-2016 [10] offers detailed guidance on security analysis V&V activities in Annex J.3. According to Annex J.3 [10], the security analysis should consider the following elements:

- The context of the system
- The system of interest and its elements, threats, vulnerabilities, and countermeasures
- Trade-offs between techniques, operations, and management to address security requirements
- Identification of threats (These threats may be natural (e.g., inclement weather, earthquakes), human (e.g., unintended or malicious), or environmental (e.g., chemical leak, power loss).

The V&V security analysis task is typically performed using threat-based analyses and is conducted in parallel with the project-level system security risk assessments to ensure alignment between verification activities and the overall system security posture. The assessments include 1) Identification of threats, 2) Identification of system vulnerabilities, 3) Evaluation of controls needed to prevent threats from exercising a potential vulnerability, 4) Evaluation of the likelihood of a threat, 5) Evaluation of the impact of a security breach or security policy violation [10]. Based on the security risk assessments, security control requirements are established, aiming to mitigate risks to levels acceptable to stakeholders. For security requirements with high integrity levels or severe security impact, rigorous V&V activities are necessary. Then, for such "critical" security requirements, the V&V security analysis includes the following activities:

- Traceability of critical requirements through the life cycle
- Evaluation of potential threat sources and vulnerabilities
- Evaluation of architectures and designs to determine whether security functions meet required capabilities
- Application of verification methods such as analyses (e.g., statistical analyses), inspections, demonstrations, and tests (e.g., vulnerability scanning, penetration testing)
- Review of the residual security risks

2.3 IEC 62645:2019 Standard

IEC 62645 [11] is an international standard that specifies security requirements for protecting I&C programmable digital systems in nuclear power plants against cyberattacks. The standard encompasses a system-level security lifecycle and complements the

Table I: SDOE V&V vs Cybersecurity V&V

Table I: SDOE V&V vs Cybersecurity V&V

	SDOE V&V	Cybersecurity V&V
Objective	To verify and validate that the development, testing, and operational processes and environments (including facilities, tools, networks, and procedures) are adequately protected against unintended non-malicious acts and threats.	To verify and validate that system-required threat controls and protective measures achieve a secure level of protection against malicious threats, providing sufficient assurance.
Analysis	Threat/Vulnerability Analysis for Security Risk Assessment	Threat/Vulnerability Analysis for Security Risk Assessment
Criteria	Security degree (or Integrity level, Security level)	Security degree (or Integrity level, Security level)
Relevant Regulations & Standards	NRC RG 1.152 Rev.4 [6], IEEE 7-4.3.2 [8], IEEE 1012 (2004, 2012, 2016) [7],[9],[10]	RG 5.71(NEI 08-09) [4], IEEE 1012 (2004, 2012, 2016) [7],[9],[10], IEC 62645 [11]
Representative V&V Tasks	- Evaluation of SDOE procedures - Assessment of development environment security - Verification of operational environment security	- Verification of cybersecurity control effectiveness - Evaluation of mitigation measures
V&V Methods	- Physical/logical separation inspection - Static/dynamic vulnerability scanning - Procedural and access audits - Hardening of development/testing tools	- Static/dynamic vulnerability scanning - Penetration testing - Simulator testing (e.g., HILS) - Configuration and patch status scanning
Key Deliverables	SDOE Assessment Report	Security Analysis Report, Anomaly Report

system safety lifecycle described in IEC 61513 [12] by providing an integrated management framework that incorporates cybersecurity considerations. With regard to security V&V, this standard provides detailed descriptions of both the security requirements and the assigned security degree. The security requirements for I&C programmable digital systems can be categorized into three dimensions: 1) programme level, 2) system level, 3) security control level across the system lifecycle. Here, the security requirements are the baselines for security V&V. The security degree of an I&C programmable digital system is assigned from S1 to S3 according to the potential maximum impact on safety and system performance in the event of a successful cyberattack. Consequently, security V&V activities can be applied in a graded manner in accordance with the assigned security degree.

3. Considerations from Regulatory and Standardization Trends on Security V&V

This section presents considerations and insights based on regulatory and standardization trends on security V&V discussed in Section 2. From a security perspective, V&V activities aim to

- 1) Verify that the required threat controls are properly implemented in the system and provide the intended level of protection against identified vulnerabilities.
- 2) Evaluate from a process perspective whether development, V&V, and operational activities are carried out in accordance with established safety–security procedures.

Based on these objectives, the security V&V can be categorized into 1) cybersecurity V&V targeting malicious attacks, and 2) SDOE V&V addressing accidental and non-malicious events, as summarized in Table I. It should be noted that while the NRC provides regulatory guidance for the SDOE V&V framework within safety systems, corresponding guidance for cybersecurity-focused V&V is not yet established. Nevertheless, international industrial standards (IEEE, IEC) provide guideline trends for the cybersecurity V&V. The following primary considerations and insights can be drawn from these trends:

- The rigor of security V&V activities should vary according to the assigned security degree (or integrity level, security level).
- The security V&V activities could be based on threat analyses, with security risk assessment conducted in parallel to V&V activities.
- Traceability of critical security requirements associated with rigor security degree may be maintained throughout the system lifecycle.
- Security analysis report may serve as an output of individual security V&V process, and it can be incorporated into single security analysis report.
- The impact of security control measures on safety systems should be examined. Security controls shall not affect the performance, reliability, or availability of safety systems.

- It may be beneficial for security V&V activities to be conducted by an independent organizational entity, which could help maintain objectivity and credibility.

4. Conclusions

This paper examined trends in security V&V for nuclear facilities to extract relevant considerations and insights. The review of NRC regulatory guidelines indicated that the NRC framework primarily addresses SDOE V&V focused on unintended and accidental events. Nevertheless, industrial standards provide guidance on security V&V encompassing both unintended and malicious events. These standards offer useful references that may inform the development of security V&V approaches. The considerations derived from this analysis could contribute to the formulation of a regulatory framework for security V&V.

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 Nuclear Security Series No. 33-T, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, International Atomic Energy Agency, Vienna, 2018.
[2] IAEA Nuclear Security Series No. 17-T, Computer Security Techniques for Nuclear Facilities, International Atomic Energy Agency, Vienna, 2021.
[3] IAEA Nuclear Energy Series No. NR-T-3.30, Computer Security Aspects of Design for Instrumentation and Control Systems at Nuclear Power Plants, International Atomic Energy Agency, Vienna, 2020.
[4] RG 5.71, Rev. 1, Cyber Security Programs for Nuclear Power Reactors, U.S. Nuclear Regulatory Commission, Washington, DC, 2023.
[5] RG 1.168, Rev. 2, Verification, Validation, Reviews, and Audits for Digital Computer Software used in Safety Systems of Nuclear Power Plants, U.S. Nuclear Regulatory Commission, Washington, DC, 2013.
[6] RG 1.152, Rev. 4, Criteria for Programmable Digital Devices in Safety-Related Systems of Nuclear Power Plants, U.S. Nuclear Regulatory Commission, Washington, DC, 2023.
[7] IEEE Std 1012-2004, IEEE Standard for Software Verification and Validation, IEEE, 2004.
[8] IEEE Std 7-4.3.2-2016, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, IEEE, 2016.
[9] IEEE Std 1012-2012, IEEE Standard for System and Software Verification and Validation, IEEE, 2012.
[10] IEEE Std 1012-2016, IEEE Standard for System, Software, and Hardware Verification and Validation, IEEE, 2017.
[11] IEC 62645:2019, Nuclear Power Plants – Instrumentation and Control Systems – Requirements for Security Programmes for Computer-based Systems, International Electrotechnical Commission, 2019.
[12] IEC 61513:2011, Nuclear Power Plants – Instrumentation and Control Important to Safety – General Requirements for Systems, International Electrotechnical Commission, 2011.