Korean Nuclear Society Spring Meeting, 2025

A Review of International Cybersecurity Strategies for Nuclear Power Plants Based on IEC SC 45A Standards

Juhyung Song, Jae-gu Song, Jaekwan Park, Youngjun Lee

Korea Atomic Energy Research Institute

Corresponding author : jhsong@kaeri.re.kr

Introduction

- The increasing cyber threats to nuclear power plants have elevated cybersecurity to a global concern. With growing cybersecurity threats to nuclear power plants, harmonizing national guidelines with international standards has become increasingly important for effectively managing security risks. This paper analyzes the internationally recognized IEC SC 45A standards, specifically IEC 62645, IEC 62859, and IEC 63096, and examines their compatibility with domestic cybersecurity guidelines for nuclear facilities (KINAC/RS-015). Based on this analysis, we aim to provide directions that can enhance the international response capabilities of domestic nuclear power plants and secure competitiveness in nuclear exports.

Fig 1. Overview of IEC SC45A security standard series: IEC 62645, IEC 62859, IEC 63096

IEC SC 45A Standards

The IEC SC 45A standards are internationally recognized and define security requirements for instrumentation and control (I&C) systems in nuclear facilities. This standard series encompasses multiple frameworks related to nuclear cybersecurity. In this study, we focus on the following three key standards:

- IEC 62645: Specifies the requirements for establishing a cybersecurity management framework and security programs for the instrumentation, control, and power systems of nuclear facilities. It provides guidelines for establishing cybersecurity policies at the organizational level, clarifying responsibilities and roles, building and operating security programs, and implementing continuous risk assessment and management measures.
- IEC 62859: Deals with the requirements for coordinating the safety and security of digital I&C systems in nuclear power plants. It presents effective management strategies through integrated safety security design.
- IEC 63096: Offers detailed security controls based on the management framework defined in IEC 62645. This provides concrete security measures for the practical implementation of cybersecurity in nuclear facilities.

Regarding the relationship between these standards, IEC 62645 provides a framework for security programs, while IEC 63096 explains practical methods for selecting and applying security measures based on this framework. Both standards maintain compatibility in applying security measures according to security levels (BR, S1, S2, S3). IEC 62859 focuses on integrating safety and cybersecurity, and when used with IEC 62645 and IEC 63096, it enhances the overall safety and security of I&C systems. This study focuses on IEC 62645, which is centered on management systems and policies, and analyzes its compatibility with domestic guidelines (KINAC/RS-015) to derive policy improvement directions for domestic nuclear facilities to comply with international standards.

Gap Analysis Approach

- With the growing importance of cybersecurity in nuclear facilities, harmonizing national regulatory guidelines with international standards remains a key challenge. To examine this relationship, this study conducts a gap analysis of the KINAC/RS-015 guidelines against the international standard IEC 62645. The analysis process is as follows:
- Firstly, the major cybersecurity management requirements and recommendations from the IEC 62645 standard document were reviewed to select analysis items. The key selected items included establishing a cybersecurity management framework, clarifying organizational responsibilities and roles, defining security levels and security management procedures, and building continuous security evaluation and risk management processes.
- Secondly, the analysis items from IEC 62645 were mapped against the corresponding items in the KINAC/RS-015 guidelines to compare them. The study evaluated how well the management requirements and detailed technical requirements in the domestic guidelines aligned with the major requirements of international standards.
- Thirdly, through this analysis, the differences were identified via gap analysis. Rather than determining explicit deficiencies or mandatory supplementation in the domestic guidelines, the study focused on recognizing the variances between the two sets of standards. By understanding these differences, this research seeks to explore cybersecurity perspectives from the EU and other international contexts, thereby providing insights into the approach to cybersecurity management within nuclear facilities abroad.

Consequently, the gap analysis serves as a practical tool to objectively examine the relationship between IEC 62645 and KINAC/RS-015, aiming to enhance the understanding of international cybersecurity practices and their implications for domestic nuclear facilities.

Results and Discussion

The results of the gap analysis for compatibility between the major requirements of IEC 62645 and KINAC/RS-015 are as follows:

- Cybersecurity Management Framework and Program Establishment: KINAC/RS-015 clearly specifies the requirements for establishing and operating a management framework and security programs, demonstrating compatibility with international standards.
- Organizational Responsibilities and Roles: KINAC/RS-015 clearly defines the responsibilities and roles not only for operating organizations but also for contracted companies, meeting the requirements of international standards.
- Cybersecurity Levels and Defense Structure: KINAC/RS-015 requires multiple security boundaries and clear compartmentalization for systems and networks, aligning with the requirements of international standards.
- Security Evaluation and Risk Management Framework: IEC 62645 outlines specific methodologies, evaluation cycles, and procedures for security assessments, whereas KINAC/RS-015 emphasizes the importance of security evaluations in general terms without detailing procedural guidelines.
- Continuous Security Evaluation and Risk Management: Both KINAC/RS-015 and IEC 62645 underscore the significance of regular security evaluations. IEC 62645 provides structed criteria regarding evaluation cycles, methodologies, and risk management approaches, while KINAC/RS-015 maintains flexibility by emphasizing principles without prescribing specific detailed guidelines.

The analysis shows that domestic guidelines largely reflect the major requirements of IEC 62645. However, gaps exist in the detailed standards for security evaluation and risk management methodologies, as well as in the integrated management of safety and security. Addressing these gaps will be beneficial for securing international credibility in nuclear exports.

This analysis highlights areas where KINAC/RS-015 aligns with IEC 62645 but also identifies areas needing improvement, particularly in providing detailed procedures for security assessments and integrating safety and security management. Enhancing these aspects will contribute to strengthening the international competitiveness of domestic nuclear power plantsp analysis serves as a practical tool to objectively examine the relationship between IEC 62645 and KINAC/RS-015, aiming to enhance the understanding of international cybersecurity practices and their implications for domestic nuclear facilities.

Conclusions and Future Work

This study conducted the gap analysis between the international cybersecurity standard IEC SC 45A and the domestic guideline KINAC/RS-015. The results confirmed that the domestic guidelines and the international standards largely present similar requirements. However, gaps were identified in the detailed standards for security evaluation and risk management methodologies, as well as in the integrated management of safety and security. These findings are significant for enhancing the efficiency and effectiveness of cybersecurity management in nuclear power plants and for fostering mutually complementary development between domestic guidelines and international standards. Therefore, systematic and specific policy improvements could be considered to address these gaps, particularly in areas where clearer guidance may enhance practical implementation. However, considering that RS-015 functions as a regulatory guideline that inherently allows for flexible implementation, it is important to further examine whether the observed differences alone provide sufficient grounds for such changes. Continued efforts to harmonize domestic guidelines with international standards may contribute to improving the applicability and credibility of cybersecurity practices in the nuclear sector.

- Future research plans to compare and analyze the IEC SC 45A standards with the recently published Network and Information Systems Security (NIS2) directive in the EU. This will facilitate in-depth discussions on domestic policy responses to changes in the international cybersecurity environment. The goal is to support further improvements in domestic nuclear facility security guidelines and the establishment of internationally applicable nuclear cybersecurity policies. Additionally, based on these research findings, a strategic roadmap will be developed to address potential international regulatory issues related to cybersecurity that may arise during future nuclear exports.

Acknowlegment

This work 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).