A Study on the Coordinating of Safety Design Regulations and Cybersecurity Technical Requirements for Nuclear Power Plants

Ieck-Chae Euom [a*], Joon-Seok Kim [b]
[a]*Department of Data Science, Chonnam National University, Gwangju 61186, Republic of Korea*
[b]*System Security Research Center, Chonnam National University, Gwangju 61186, Republic of Korea*
[*]*Corresponding Author : icelaken@ chonnam.ac.kr*

***Keywords : Nuclear Power Plant, Safety, Security**

1. Introduction

Digitization and enhanced network connectivity (Instrumentation & Control, I&C) systems have greatly improved the operational efficiency and safety of nuclear power plants. However, these technological advances have also increased vulnerabilities against cyber threats. The process of integrating software within a safety-critical infrastructure presents attackers with the opportunity to exploit software vulnerabilities, which lead to design flaws, bugs, and security issues within the system. This situation demonstrates the need for current systems to meet and manage new cybersecurity requirements in addition to existing safety-oriented approaches[1].

The fields of safety and security have grown largely independently over the decades, each evolving their own principles, tools, and methodologies. However, it is necessary to consider synergies, interactions, and potential side effects when both fields are applied to the same I&C system and architecture. IEC 62859 describes the requirements for safety and security in nuclear facilities. It shows how security requirements can be met within a safety-based basic design environment[2].

This study investigated the integration of the security requirements of IEC 62859 with the security requirements of the Korean RS-015. Based on existing research on the integrated consideration of safety and security for I&C architectures in nuclear power plants, we rethink the balance in this area and propose an approach to the overall design[3].

The scope of this study is to analyze IEC 62859 and its related standards and their linkages to RS-015, the Korean nuclear facility cybersecurity standard.

2. Safety and Security Regulations for Nuclear Power Plant

This chapter analyzes the current status of domestic and foreign regulations for linking safety and security requirements of nuclear facilities.
The following Figure 1 shows the current status of domestic and international regulations on the safety and security of nuclear power plants. These regulations are used to evaluate and manage the safety and security of nuclear power plants.

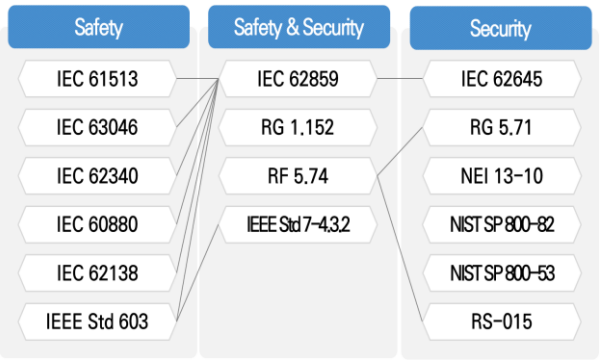

Fig. 1. Domestic and international regulatory status of nuclear power plant safety and security

2.1. Safety Regulations

The 'Safety' category consists of standards from the International Electrical and Technological Council (IEC) and the Electrical and Electronic Engineering Council (IEEE), which focus on safety.
It includes IEC 61513, IEC 63046, IEC 62340, and defines requirements for the design and operation of safety systems in nuclear power plants.

2.2. Safety and Security Regulations

The 'Safety & Security' category lists regulations and standards that require an integrated approach to safety and security. These include IEC 62859 and the U.S. Nuclear Regulatory Commission's RG 1.152, RF 5.574, and IEEE Std 7-432.
These standards acknowledge that safety and security can affect each other and emphasize that the system should be designed and evaluated in consideration of this.

2.2.1. IEC 62859

The IEC 62859 standard provides guidelines for the integrated management of cybersecurity and safety within the Instrumentation & Control (I&C) systems of nuclear power plants. It particularly emphasizes methods to coordinate safety and cybersecurity at both the overall architectural level and the individual system level. This standard includes cybersecurity measures throughout various stages of the lifecycle, including requirement definition, design, implementation, verification and validation, installation, operations and maintenance, change management, and decom missioning activities. By following these guidelines,

nuclear facilities can establish measures to manage risks while considering both safety and cybersecurity.

2.2.2. IEEE 7-4.3.2

IEEE Std 7-4.3.2 is a standard for the use of programmable digital devices within the safety systems of nuclear power plants. It emphasizes communication configurations considering safety design and addresses cybersecurity management. The standard defines the minimum functionality, performance, and design requirements necessary to ensure the reliability of digital systems and protect them from cyber threats. It aims to enhance overall safety through effective integration of safety systems, providing guidelines for cyber risk assessment and management, and maintaining cybersecurity during operations.

2.2.2. RG 1.152

RG 1.152 is a guideline from the U.S. Nuclear Regulatory Commission (NRC) on the use of digital devices in the safety systems of nuclear facilities. It covers the approach to design, implementation, verification, and operation to ensure system reliability and protect against cyber threats. Key elements for maintaining safety and security include system integration, fault tolerance, and risk management.

2.3. Security-related regulations

The 'Security' category lists regulations and standards focusing on cybersecurity. These include standards such as IEC 62645, NEI 13-10, NIST SP 800-82, NIST SP 800-53 and RS-015, which suggest how to assess and manage cybersecurity risks in nuclear facilities.

2.3.1. RS-015

The U.S. NRC published Guide 5.71, "Cybersecurity Programs for Nuclear Facilities," in 2010, and has been conducting full implementation and inspections of security measures since 2017. In South Korea, the Korea Institute of Nuclear Safety and Control (KINAC) published the RS-015 standard on cybersecurity for nuclear facilities in 2014, which provides security suggestions that should be applied technically, operationally, and administratively[4].

RS-015 has three areas: technical security measures, management security measures, and operational security measures, with a total of 101 security measures divided into 13 groups.

3. Integrate Safety and Security Regulations

In the process of exploring the relationship between IEC 62859 and RS-015, a thorough analysis was conducted using a comparative table of various international standards to identify potential connections. IEC 62859 provides guidance on how cybersecurity and safety should interact and be coordinated both at the overall architectural and individual system levels in nuclear power plants.

Specifically, the detailed analysis aimed to uncover how the cybersecurity controls proposed by IEC 62859 could potentially align with the security measures based on safety design found in RS-015. For example, the technical controls like logical access control and the use of cryptography outlined in IEC 62859 could complement the access control and system hardening measures detailed in RS-015. Such an intersection may help in reinforcing safety design through a cybersecurity lens.

Table 1 is a comparative analysis of the relationships between international standards concerning the integration of cybersecurity and safety in nuclear power facilities. This table methodically contrasts the scope, key features, lifecycle phase approaches, technical and operational controls, as well as management control methods of IEC 62859, RG 1.152, IEEE Std 7-4.3.2,

Table 1 Comparative Analysis of International

Standard/ Regulation	Scope	Key Features	Lifecycle Phase	Technical Controls	Operational Controls	Management Controls	Intersections
IEC 62859	Integration of safety and cybersecurity in nuclear power plants	Coordinating safety and cybersecurity	Design, operation	Logical access control	Change management	System and service acquisition	IEC SC 45A subdocument, leveraging various IEC standards
RG 1.152	Criteria for computers in safety systems of nuclear power plants	Standards for the use of programmable digital devices in safety-related systems	Design, implementation, verification, operation	System integration, fault tolerance and resilience	Human factors management, education and training programs	Risk assessment and management approaches	Connections with other standards like IEC 62859 and IEEE Std 7-4.3.2
IEEE Std 7-4.3.2	Use of programmable digital devices within safety systems of nuclear power plants	Complementary to IEEE Std 603, and design requirements for safety systems	Design, implementation, verification, operation	System integration and reliability assurance	Maintenance of cyber security during operation	Cyber risk assessment and management	Security requirements linkage with IEC 62859, RG 1.152
RS-015	Cybersecurity for nuclear facilities	Specific to regulatory framework, technical requirements for compliance	Comprehensive coverage	Access control, system hardening	Personnel security, awareness and training	Security assessment	Standards for Cybersecurity Measures at Domestic Nuclear Facilities

and RS-015. For instance, IEC 62859 outlines the integration of cybersecurity within the safety systems of nuclear power plants, RG 1.152 sets forth criteria for computers in safety systems, IEEE Std 7-4.3.2 addresses complementary standards for the use of programmable digital devices, and RS-015 specifies technical compliance requirements within the regulatory framework for cybersecurity in nuclear facilities. The insights gained from Table 1 will contribute to standardizing cybersecurity measures for domestic nuclear facilities.

3.1. Access Control Requirements

In this chapter, we derived the linkage between the requirements to align the safety and security requirements of nuclear facilities. Based on IEC 62859, the requirements of RS-015, the Korean cybersecurity standard for nuclear facilities, were analyzed in conjunction with each other.

The IEC 62859 standard stipulates safety and cybersecurity measures for nuclear power plant I&C systems, which closely relate to the Technical Controls section of the KINAC RS-015 standard. Each technical control in RS-015 correlates with life cycle activities in the IEC standard, providing detailed guidance on access control, communication protection, and authentication. Additionally, specific technical aspects of the IEC standard, such as logical access control, software modification, and system auditing, are linked with corresponding items in RS-015.

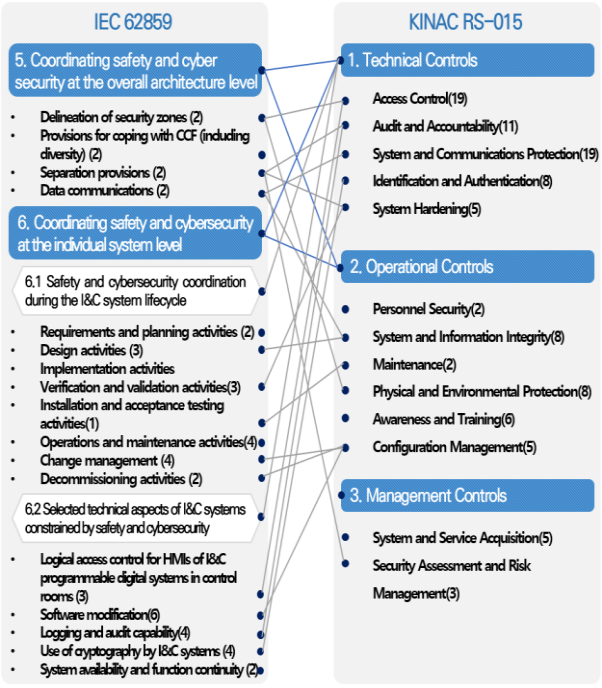

Fig. 2. Derive RS-015 security requirements to mutually satisfy safety and security objectives in nuclear facilities based on IEC 62859

3.1. Access Control Requirements

The IEC 62859 standard stipulates safety and cybersecurity measures for nuclear power plant I&C systems, which closely relate to the Technical Controls section of the KINAC RS-015 standard. Each technical control in RS-015 correlates with life cycle activities in the IEC standard, providing detailed guidance on access control, communication protection, and authentication. Additionally, specific technical aspects of the IEC standard, such as logical access control, software modification, and system auditing, are linked with corresponding items in RS-015.

3.2. RS-015 Operational Controls

IEC 62859 centers on safety and cybersecurity coordination throughout the I&C system lifecycle, while KINAC RS-015's 'Operational Controls' outline supporting security operations. 'Personnel Security' and 'Awareness and Training' emphasize the significance of personnel in operations and maintenance, 'System and Information Integrity', and 'Configuration Management' underscore the importance of managing system changes and configurations. 'Maintenance' and 'Physical and Environmental Protection' indicate the necessity of system verification and physical environment protection.

3.3. RS-015 Management Controls.

IEC 62859 emphasizes the coordination of safety and cybersecurity within the overall architecture, closely related to 'Management Controls'. KINAC RS-015's 'Management Controls' address the cyber security management aspects of nuclear facilities, including 'Decommissioning activities', encompassing management activities for establishing system requirements, planning in the design phase, and ensuring safety post-operation.

4. Conclusion

This study analyzed the domestic and international nuclear facility regulations and studied the integration of IEC 62859 safety-based security requirements with RS-015, the Korean nuclear facility security standard.

As a future research project, we will study the implementation of detailed technical, operational, and managerial security measures.

Acknowledgement

"This work was supported by Institute for Information & communications Technology Planning & Evaluation(IITP) grant funded by the Korea government(MSIT)(No.2022-0-01203, Regional strategic Industry convergence security core talent training business)

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. 2022R1G1A1010506).

REFERENCES

[1] Linnosmaa, Joonas, et al. Security and Safety Integration for the Nuclear Instrumentation and Control Systems. In: 2022 IEEE 27th International Conference on Emerging Techno logies and Factory Automation (ETFA). IEEE, pp. 1-7. 2020.

[2] IEC, “Nuclear power plants — Instrumentation and control systems — Requirements for coordinating safety and cybersecurity,” IEC 62859:2016, 2016.

[3] KINAC/RS-015.01, “Regulatory Standard on Cyber Security for Nuclear Facilities”, December, 2014

[4] US NRC Regulatory Guide 5.71, “Cyber Security Programs for Nuclear Power Facilities,” 2010