Enhancing the Safety-Security Interface: A Comparative Analysis of the U.S. NRC's ROP and South Korea's Regulatory Framework with a Focus on Cybersecurity

Jinho Ryu[a*] Aram Kim[a], Kihaeng Nam[a]
[a]*Korea Institute of Nuclear Non-proliferation and Control (KINAC).,*
1418 Yuseongdaero, Daejeon, Korea
[*]*Corresponding author: jhryu@kinac.re.kr*

Abstract

This paper compares the regulatory frameworks for nuclear safety and security in the United States and South Korea, with a focus on cybersecurity. While both frameworks share common objectives, they differ in organizational structure and focus. The paper suggests that South Korea could benefit from adopting a more integrative approach to cybersecurity, drawing inspiration from the U.S. Nuclear Regulatory Commission's Reactor Oversight Process (ROP). Meanwhile, the U.S. could explore ways to further specialize and strengthen specific safety and security aspects within the ROP, drawing from the experiences of Korean regulatory bodies. The paper concludes that by addressing these opportunities and fostering collaboration, both countries can strengthen their nuclear safety and security measures and contribute to global efforts in this critical area.

1. Introduction

The incidents of Fukushima Daiichi in 2011 and the increased awareness of potential terrorist threats to nuclear facilities, including cyberattacks, have highlighted the need for enhancing nuclear safety and security worldwide [1]. The safe and secure operation of nuclear power plants is vital for public health, environmental protection, and the credibility of the nuclear industry [2]. Therefore, regulatory bodies worldwide have been striving to establish effective frameworks to ensure the sufficient level of safety and security in the operation of nuclear power plants, including robust cybersecurity measures [3].

This paper compares two such frameworks: the U.S. Nuclear Regulatory Commission (NRC)'s Reactor Oversight Process (ROP), which is a systematic and risk-informed approach for ensuring reactor safety, radiation safety, and safeguards, and South Korea’s regulatory framework under the guidance of the Korean Nuclear Safety and Security Commission (NSSC), which includes the Korean Atomic Energy Act and the regulations for nuclear safety and security.

2. U.S. NRC’s Reactor Oversight Process (ROP)

2.1 Overview of the ROP

The U.S. Nuclear Regulatory Commission (NRC) established the Reactor Oversight Process (ROP) as a risk-informed, performance-based regulatory framework to monitor and evaluate the safety and security performance of commercial nuclear power plants [4]. The ROP was implemented in 2000 to provide a more objective, predictable, and transparent approach to overseeing plant performance.

2.2 Components of the ROP

As shown in Figure 1, The ROP framework consists of mission, strategic performance areas, cornerstones, and cross-cutting areas. The performance areas cover reactor safety, radiation safety,

and safeguards, encompassing both safety and security aspects. Under the ROP, the overall performance evaluation of each nuclear power plant is based on two main inputs: the significance determination information from NRC inspection findings, and the Performance Indicator (PI) information for each selected area [5]. The ROP includes seven cornerstones, each represented by a corresponding PI, which are later utilized in the comprehensive plant performance evaluation.

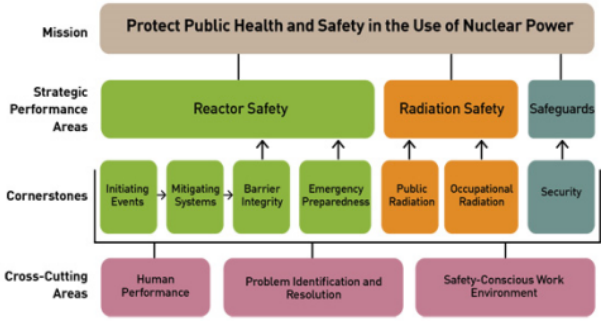

Fig. 1. Reactor Oversight Framework [4]

2.3 Integrated Safety-Security Framework in ROP

The ROP's strategic performance areas and cornerstones enable an integrated safety-security approach that promotes the organic exchange and application of safety and security-related information1. By ensuring that safety and security aspects are interwoven throughout the ROP, the framework can effectively address potential cybersecurity risks and other related concerns that may impact nuclear plant operations.

2.4 Significance of Cybersecurity in the ROP

The importance of cybersecurity is well treated in the ROP framework to maintain the safety and security of nuclear power plants. Cybersecurity is a cross-cutting area that affects various aspects of plant performance, such as physical protection, emergency preparedness, etc. Therefore, it is essential to incorporate cybersecurity into the regulatory process as part of the integrated safety-security framework. It ensures that cybersecurity is incorporated into the regulatory process as part of the integrated safety-security framework. This approach facilitates continuous monitoring and evaluation of cybersecurity measures, with evaluation results being publicly announced every six months. Consequently, this provides stakeholders with a transparent and objective understanding of the safety and security status of nuclear facilities, including their resilience against potential cyber threats.

3. South Korea's Regulatory Framework

3.1 Overview of South Korea's Regulatory Framework

South Korea's regulatory framework for nuclear safety and security consists of two main organizations, the Korea Institute of Nuclear Nonproliferation and Control (KINAC), and the Korea Institute of Nuclear Safety (KINS) and These organizations are responsible for establishing guidelines and enforcing regulations for the safe operation of nuclear power plants. Above these two organizations, the Nuclear Safety and Security Commission (NSSC) exists, overseeing and coordinating their efforts. This chapter provides an overview of the roles and responsibilities of KINAC, KINS, and NSSC in South Korea's nuclear regulatory landscape.

3.2 Roles and Responsibilities

KINAC is an independent expert organization responsible for overseeing nuclear security and nonproliferation in South Korea. Its main functions include establishing and implementing security regulations for nuclear facilities and materials, ensuring compliance with international nonproliferation agreements, conducting security inspections and assessments of nuclear facilities, and providing training and technical support to enhance security at nuclear facilities.

KINS, on the other hand, is responsible for ensuring nuclear safety in South Korea. Its primary tasks include developing and maintaining safety regulations and guidelines for nuclear facilities, reviewing the safety analysis reports submitted by licensees, conducting independent safety assessments and inspections of nuclear facilities, and providing technical support to the NSSC in the development of nuclear safety policies.

The NSSC is the primary regulatory body overseeing KINAC and KINS. It is responsible for coordinating the efforts of these organizations and ensuring a comprehensive approach to nuclear safety and security in South Korea. The NSSC's main responsibilities include developing and implementing national policies related to nuclear safety and security, reviewing and approving safety and security regulations established by KINAC and KINS, coordinating the regulatory activities of KINAC and KINS, and ensuring effective communication and collaboration between KINAC and KINS, as well as with international organizations and other stakeholders.

4. Comparative analysis

4.1 Overview of Similarities and Differences

Both the U.S. NRC's ROP and South Korea's regulatory framework share common objectives in ensuring the safe and secure operation of nuclear power plants. Key similarities between the two frameworks include the use of review, inspections, and assessments to evaluate plant performance regarding security or safety, identify potential issues, and enforce compliance with regulations. Furthermore, both frameworks recognize the importance of collaboration and communication among stakeholders, including international organizations, for the exchange of best practices and enhancement of their regulatory efforts.

In terms of organizational structure, the U.S. NRC functions as a single, independent regulatory body responsible for overseeing nuclear safety and security, while South Korea adopts a more decentralized approach with KINAC and KINS, and the NSSC sharing responsibilities for regulation and oversight. This structural difference leads to variations in how each country approaches the division of tasks and responsibilities, coordination, and decision-making processes.

The ROP is structured around seven cornerstones, as described in Fig. 1., covering various aspects of nuclear safety and security. These cornerstones ensure that the U.S. NRC addresses all critical areas in a balanced manner. In contrast, South Korea's framework is divided into the distinct roles of KINAC and KINS, with the NSSC overseeing and coordinating their efforts. This division of roles results in a more specialized focus on specific safety and security aspects, but it may also lead to potential gaps or overlaps in addressing certain concerns.

Another key difference lies in the enforcement and regulatory response mechanisms. The U.S. NRC's ROP employs a graded approach, where the level of regulatory scrutiny increases with the significance of identified performance issues. South Korea's regulatory framework also involves a graded approach [6, 7], but the specifics of the enforcement mechanisms and the criteria for escalating regulatory actions may differ in each organization (KINAC and KINS), leading to variations in how each organization responds to safety or security concerns.

4.2 Implications and Opportunities for Enhancing SSI, with a Focus on Cyber Security Plan

The differences in organizational structure and focus of the regulatory programs between the U.S. NRC's ROP and South Korea's framework present opportunities for enhancing the safety-security interface, particularly in the area of cybersecurity. In the U.S., the Cyber Security Plan (CSP) is reviewed as an integrated part of the licensing process, according to U.S. NRC Regulatory Guide 1.70 [8] and NUREG-0800 [9]. The CSP is incorporated into Chapter 13 of the Safety Analysis Report (SAR), ensuring that cybersecurity measures are embedded within the overall licensee's quality assurance system.

In contrast, South Korea's regulatory framework does not include a CSP review during the licensing process. Instead, it requires an independent review and approval of the CSP separate from the licensing process. This separation results in a weaker interface between the overall nuclear licensee's quality assurance system and cybersecurity, as they operate independently from one another.

The centralized approach under the NRC offers more streamlined coordination and decision-making, while South Korea's decentralized structure could allow for greater specialization and focus on specific safety and security aspects. However, the lack of interfaces between safety and security in South Korea's framework may lead to potential gaps or overlaps in addressing cybersecurity concerns.

One opportunity for improvement is to learn from each other's experiences and best practices. For instance, it could be beneficial for South Korea to consider implementing a more integrative approach to cybersecurity, drawing inspiration from the U.S. NRC's ROP. Such an approach focuses on a well-rounded and balanced strategy for addressing concerns related to safety and security. On the other hand, the U.S. could explore ways to further specialize and strengthen specific safety and security aspects within the ROP, drawing from the experiences of KINAC and KINS.

Another opportunity lies in fostering greater collaboration and communication between the U.S. NRC, KINAC and KINS, and the NSSC, as well as with other international organizations. By sharing knowledge, experiences, and best practices, both countries can continue to enhance their respective nuclear safety and security regimes, including their approaches to cybersecurity, while also contributing to global efforts in this critical area.

5. Conclusion

This research paper provided a comparative analysis of the U.S. NRC's ROP and South Korea's regulatory framework, focusing on their approaches to nuclear safety and security. Despite sharing common objectives and elements, differences in organizational structure and focus present opportunities for improvement in both countries.

In conclusion, the comparative analysis offers valuable insights into enhancing the safety-security interface in the U.S. and South Korea. By addressing these opportunities and fostering collaboration, both countries can strengthen their nuclear safety and security measures, ensuring the safe operation of nuclear power plants and contributing to global efforts in this critical area.

Acknowledgement

This work was supported by the Nuclear Safety Research Program through the Korea Foundation of Nuclear Safety(KoFONS) using the financial resource granted by the Nuclear Safety and Security Commission(NSSC) of the Republic of Korea. (No. 2106013)

REFERENCES

[1] K. Siewert, “INSAG Forum Discusses Safety-Security Interface Developments and Challenges,” *IAEA*, Sep 2019.
[2] “Integrated Regulatory Review Service Mission to the United States”, *U.S. NRC*, ML112510464
[3] NY Lee et al., “Development of the 3S interface in the regulatory point of view R&D Report”, *KINAC*, Apr 2016.
[4] “Reactor Oversight Process (NUREG/BR-0508, Revision 1)”, *U.S. NRC*, Apr 2016.
[5] HJ Lee et al., “Trend Analysis of Risk-Informed and Performance-based Regulation for Security Area Application”, *KINAC*, Oct 2016.
[6] Dh Kim., “Current Status of Domestic Risk-informed regulations”, *KINS*, May 2021.
[7] SM Lim, "Risk-Informed Based Graded Approach and Consequence Assessment on Cyber Security Measure in Nuclear Facilities.", *KINAC,* May 2019.
[8] “Regulatory Guide 1.70, Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants”, *U.S. NRC*, 1978
[9] “NUREG-0800 Ch. 13.6.6, 'Cyber Security Plan”, *U.S. NRC*, 2010