A Study on Nuclear Safety-Security Interface Management

Min Baek, Sunghun Oh *
Korea Institute of Nuclear Non-proliferation and Control, 1534 Yuseong-daero, Daejeon, 34154, Korea
**Corresponding author: k067osh@kinac.re.kr*

1. Introduction

As the security level of nuclear facilities has increased since the 9.11 terrorist attacks in 2001, the importance of physical protection and cyber security has been magnified. The security of nuclear facilities has become a key factor to be considered in the regulation of nuclear facilities along with nuclear safety.

As the public's interest in cyber-attacks on nuclear power plants increases due to cases of cyber-attack attempts on nuclear power plants, there are calls for securing safety of nuclear power plants by strengthening cyber security.

Nuclear safety and security have a common goal of protecting the public and the environment from radiation hazards, and their defense-in-depth (DiD) strategy such as prevention, protection, mitigation and accident response are the same. However, differences exist in prevention and response methods due to different causes of problems.

Thus, it is necessary to manage the Integrated Safety-Security Interface (SSI) to reduce safety-security conflicts and achieve the common purpose for safety regulations. Considering the above points, this paper will analyze the current status and problems of the nuclear safety-security interface management and suggest some improvement plans.

2. Trends of Nuclear Safety-Security Interface Management

2.1 International Trends

Recognizing the importance of SSI, the IAEA adopted a resolution at the IAEA General Conference in 2008 to strengthen cooperation in safety/security activities and prevent radioactive terrorism of nuclear materials. In January 2011, INFCIRC/225, a recommendation document for physical protection, was amended to recommend that it is necessary to review and supplement matters that conflict between safety and security in the design phase of a new nuclear power plant. In addition, it advised that in nuclear materials and nuclear facilities safety and security should supplement each other.

IAEA SSI-related documents (INSAG-24) also provide differences between safety and security and SSI measures throughout the whole cycle (site selection, design, construction, operation and decommissioning).

The safety design requirements such as defense-in-depth, redundancy and diversity are areas that create synergies in SSI, while the barrier/fence is the conflicting areas because it can delay safe evacuation in emergency situations.

The Nuclear Security Series (NSS No. 33-T), published by the IAEA, states that safety measures and security measures should be designed and implemented in an integrated manner between two areas, and security measures should not harm safety and safety measures should be kept from harming security.

It also stipulates that security measures should not degrade the ability to perform unintended malfunctions or safety functions. In addition, safety-security interface requirements are specified in the IAEA's specific safety requirements [SSR-2/1 (design) and SSR-2/2 (operating)], concerning the design and operation of nuclear facilities.

In the United States, changes in the social environment following the 9.11 terrorist attacks led to the need to improve the SSI's framework from three major perspectives. In other words, the improvements of the system to strengthen security measures for nuclear facilities include redefining DBT, collision by aircraft and cyber security measures. Among these, improving the system for SSI requires an assessment of possible conflicts between safety and security measures at particular facilities.

The NRC enacted 10 CFR Part 73.58 (Safety-Security Interface Requirements for Nuclear Power Plants) in 2009, and in June of the same year, Reg. Guide 5.74 (Safety-Security Interface Management) was established to manage SSI.

This regulatory guide requires that the licensee shall assess and manage the potential for adverse effects on safety and security, including the site emergency plan, before implementing changes to configurations, facility conditions and security.

2.2 Domestic Trends

As a follow-up measure to the 2012 Seoul Nuclear Security Summit, Korean government established a plan for nuclear safety and nuclear security interface. In December 2013, the *Enforcement Decree of the Act on Physical Protection and Radiation Emergency* was amended to allow nuclear operators/utilities to "evaluate and take complementary measures to assess the safety effects of design, operation and modification of physical protection system on nuclear facilities."

In November 2105, The Nuclear Safety and Security Commission (NSSC) was required to take both safety and security into consideration and re-designate vital

areas regarding construction and operating nuclear power plants. The Korea Institute of Nuclear Non-proliferation and Control (KINAC) established the Technical Standards (RS-107) for the establishment of vital areas in July 2017 to conduct an assessment on the re-establishment of vital areas.

In addition, the KINAC Cyber Security Technical Standard (KINAC/RS-015) stipulates that cyber security measures should be assessed for adverse effects on safety, security, and emergency response (SSEP) functions or performance before any changes in critical digital assets (CDA) and, more specifically, the security analysis including SSI.

The Korea Institute of Nuclear Safety (KINS) has developed a digital computer-based regulatory guideline (KINS/RG-N08.13), which is used for the safety evaluation of new and operating nuclear power plants. This guidance is used to assess whether the software of a digital computer system does not include unnecessary or undocumented functions, and ensure that events initiated by inadvertent access, etc., do not impede the reliable operation of the safety system. In other words, KINS is verifying the security development and operational environment (SDOE) for the digital-based safety grade I&C system on the safety side.

3. Nuclear Safety-Security Interface Management

3.1 Nuclear Safety-Security Interface

According to the IAEA document's definition, nuclear safety is the achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in protections of workers, the public and the environment from undue radiation hazards. On the other hand, nuclear security is the prevention and detection of, and response to theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities.

On the SSI management side, factors that should be considered in determining whether changes to facilities, design, configuration, and arrangement adversely affect safety or security include reduced system reliability or utilization, increased response time for emergency/ security personnel, impeding detection and evaluation functions, and reduced effectiveness of security plans.

In the case of nuclear safety, the safety assessment is focused on risks arising from unintended events initiated by natural occurrences such as earthquakes, floods, typhoons, etc., internal events such as fire, hardware failure, etc., or unintended events caused by operator errors. However, in the case of nuclear security, the security assessment is focused on risks or events arising from malicious intent, such as theft/deception of nuclear or radioactive materials, sabotage or unauthorized access.

Table I: Comparison of Nuclear Safety and Security

Category	Nuclear Safety	Nuclear Security
Purpose	Prevention of damage to the general public and the environment from radiation hazards and mitigation of results (minimization)	
Evaluation Targets	Assessment of risk arising from unintended events initiated by natural occurrences (earthquakes, flooding) -internal events (fire, pipe breakage, loss of power) -hardware failures -human mistakes, etc.	Assessment of risk or events feared arising from malicious acts such as -nuclear material / radioactive substances theft -sabotage -unauthorized access, etc.
Characteristics	-Transparency of information -Secure accessibility	-Disclosure of information -Restricted access

These differences between nuclear safety and security often lead to conflicts between each other in carrying out each one efficiently. As mentioned earlier, nuclear safety and security are only different means, but with the same objectives. Achieving the common objectives of nuclear safety and security requires seamless coordination and management between nuclear safety and security. Therefore, the main issue is how to ensure safety by harmoniously coordinating and managing safety-security issues.

3.2 Status and Problems of SSI Management

Looking at the interface between nuclear safety and cyber security, the digitalization of the instrumentation and control systems of nuclear power plants continues to expand, and with the rapid development of IT technologies, new types of cyber threats are increasing.

The IAEA Safety Document (NSS No. 33-T) specifies that before applying security measures to the digital I&C system, the system's reliability, the effect of applying a single failure criterion to operation and operation of the safety should be evaluated, so that cybersecurity measures do not adversely affect the safety functions and the performance of the I&C system.

If a laptop is brought in for verification of safety functions of the plant, performance test and repair, it can become a malicious code inflow path and be vulnerable to cyber threats. In Article 7 of the *Enforcement Decree of the Act on Physical Protection and Radiation Emergency*, nuclear power operators are required to evaluate and supplement the effects of security measures and their changes on safety, but there is no procedure to confirm them. In addition, security measures that adversely affect safety are not identified and analyzed, and evaluation methodologies are not prepared to identify and evaluate adverse effects.

Therefore, there is a possibility that safety functions and performance may be degraded due to cyber security measures, and there may be a possibility that cyber threats will increase due to safety requirements.

KINS is responsible for safety-related tasks under the *Nuclear Safety Act*, and KINAC is responsible for

physical protection-related tasks, including cyber security under the *Act on Physical Protection and Radiation Emergency*. In other words, safety and security requirements are stipulated by other laws, and even specialized organizations are separated. Therefore, it can be said that there are vulnerable factors from SSI point of view, and there is a possibility of overlapping work or blind spots.

In regards to SSI management, the international recommendation states that sufficient cooperation is required between the responsible departments when dealing with safety and security issues in a single agency, and that the responsibilities should be clear if the responsible agencies are dualized. In addition, a system of cooperation and coordination between the two agencies should be established to coordinate and cooperate on safety and security issues. In Korea, it is necessary to establish a cooperative consultation and coordination system between the two agencies in consideration of such factors, since it is the latter case.

Moreover, there are insufficient points to say that SSI management is properly implemented due to the lack of relevant requirements, standards, and guidelines to ensure the actual implementation of SSI. The reason why the SSI problem in Korea was drawn up as an issue at the 7th IAEA Convention on Nuclear Safety (CNS) meeting and recommended for improvement is considered as such.

In terms of cyber security and safety-related management, when replacing analog systems with digital systems in operating nuclear power plants, hardware including software design changes may include matters that may affect safety or security. It is necessary that the interface review is performed systematically.

4. Conclusion

To solve the above-mentioned problems, first of all, it is necessary to prepare regulations and to supplement the sub-statutes and guidelines for the implementation of the provisions of Paragraph 5.5 of Article 7 of the *Enforcement Decree of Act on Physical Protection and Radiation Emergency*.

To implement the provisions stipulated in the current statutes, it is required to first evaluate nuclear operators/utilities according to the enforcement ordinance and then to verify the details of enforcement ordinance during the safety review and audit (physical protection, cyber security).

Second, clarifying the scope and items of SSI-related assessments by referring to 10 CFR 73.58 and Reg. Guide 5.74 is needed.

Third, identifying items of cyber security measures that may affect safety among the cyber security measures required by the digital I&C system of nuclear power plants, and assessing whether each identified item affects safety functions and performance are essential.

Fourth, stipulating SSI-related content in the *Nuclear Safety Act* or including the contents and procedures that verify it in the Safety Review Guideline (SRG) is required.

Finally, during safety review of construction and operating nuclear power plants, it is essential to prepare cooperative measures to review and verify contents related to SSI including physical protection and cyber security areas between KINAC and KINS.

REFERENCES

[1] INASG-24, “The Interface between Safety and Security at Nuclear Power Plants.”
[2] 10 CFR 73.58, “Safety/Security Interface Requirements for Nuclear Power Plants.”
[3] 10 CFR 73.54, “Protection of Digital Computer and Communication Systems and Networks.”
[4] USNRC Reg. Guide 5.74, “Managing the Safety/Security Interface.”
[5] USNRC Reg. Guide 1.152, “Criteria for use of Computer in Safety Systems of Nuclear Power Plants.”
[6] USNRC Reg. Guide 5.71, “Cyber Security Programs for Nuclear Facilities.”
[7] KINAC/GR-001, “Guideline for Evaluation of Security Regulation of Computer and Information Systems.”
[8] KINS/RG-N08.13, “Use of Computers in Safety System of NPPs.”
[9] KINAC/RS-107, “Establishment of Vital Areas.”
[10] The Act on Physical Protection and Radiation Emergency
[11] Enforcement Decree of the Act on Physical Protection and Radiation Emergency