A Study on the Improvement of 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

After the September 11 attacks in 2001 and the cyber-attacks on control systems of Iranian nuclear power plants and uranium enrichment facilities using malware STUXNET in 2010, the importance of securing nuclear facilities, including physical protection and cyber security, was greatly highlighted. Nuclear security, along with nuclear safety, has become a key factor to consider in regulating nuclear facilities.

The two events above have brought significant changes to the security program of nuclear power plants, and the growing interest in nuclear security has led to the recognition that coordination of related activities is necessary to maintain the security and safety of nuclear power plants. Actions taken to address security issues should not adversely affect safety, and management and coordination of safety improvement measures, maintenance tasks, and engineering activities to prevent the cause of security problems have become necessary.

Integrated Nuclear Safety-Security Interface (SSI) management is necessary to reduce nuclear safety-security conflicts. Improving safety-security interface problems and leveraging synergies are important for efficient and effective regulation of nuclear facilities.

In this study, we would like to examine the SSI improvement activities of the NRC and compare them with domestic conditions to propose improvement measures.

2. SSI Improvement Activities of NRC

The U.S. Nuclear Regulatory Commission (NRC) recognized the importance of nuclear safety-security interface management and has taken a few steps to improve the nuclear safety-security interface through revision of the reactor oversight framework, development of specific regulations and guidance documents, and improvement of regulatory processes.

In 2006, the NRC issued a revision to the 10 CFR Part 73 “Physical Protection of Nuclear Power Plants and Substances” to enhance the security of nuclear power plants. The regulation reflects security requirements similar to those previously imposed by the Commission orders issued after the September 11 attacks. New requirements reflecting lessons and experiences from implementing nuclear security orders, review of plant security plans, and implementation of improved security baseline inspection programs have been added.

In 2009, the NRC established the Regulatory Guide RG. 5.74 and the 10 CFR 73.58 to stipulate and implement SSI-related requirements, thereby providing specific and systematic management of SSI. This requirement stipulates that nuclear operators(licensees) establish appropriate programs for evaluation, management, and coordination of proposed changes and activities, and identify inappropriate interfaces between nuclear safety and nuclear security. The nuclear operators(licensees) take appropriate mitigation and/or compensation measures to maintain both nuclear safety and nuclear security if a potential conflict is identified.

RG. 5.74 proposes screening criteria for mitigation/ compensation measures regarding SSI assessment results on proposed change or activity as shown in Table 1. It states that mitigation/compensation measures are needed when assessment results have been drawn because conflicts in SSI can adversely affect nuclear safety or security.

Table 1. Criteria for screening mitigation/compensation measures regarding SSI assessment results

Category	Assessment Results
Physical Protection	-The proposed change or activity: ·Decreases reliability or availability of security system ·Increases the likelihood of malfunctions of security equipment or systems ·Decreases effectiveness of approved security plans or invalidation of the site protective strategy (e.g., communication, response timelines and pathways) ·Results in non-compliance with regulatory agencies’ security regulations/ requirements ·Disrupts security detection and assessment functions ·Impacts response time of emergency workers and security personnel ·Creates new target sets, change in configurations, or increase in the number of target sets ·Decreases adversary task times -The controls put in place to reduce risks during a force-on-force exercise have adverse impact on safety security interface

Cyber Security	-The proposed change of activity adversely affects cyber security controls by altering the original intended design -Cyber security activities such as installation of password protection programs cause time delays in the operation of safety-related devices
Emergency Preparedness	-The proposed change or activity: ·Adversely impacts current agreements with external local agencies to ensure offsite emergency preparedness personnel's access to the site -Emergency response actions ·Negatively impact mitigation measures that the emergency response team needs to exercise in the case of radiation emergency

The NRC incorporated nuclear safety-security interface assessments into the inspection procedures. For example, through a status inspection, the NRC inspectors collect information about the overall nuclear security and nuclear safety status of nuclear power plants, including general information on threat conditions, security guard capabilities, and security system operations. The NRC inspectors collect information on various nuclear safety and security activities through facility visits and interviews with the security personnel, and conduct inspection activities to specifically identify nuclear safety-security interface problems.

3. SSI Improvement Plan of Korea

In December 2013, the revision of the *Enforcement Decree of the Act on Measures for the Protection of Nuclear Facilities, etc. and Prevention of Radiation Disasters* stipulated that nuclear operators(licensees) should evaluate and supplement the effects of design, operation, and modification of physical protection systems on the safety of nuclear facilities. However, it is difficult to implement them in practice because there is no clear indication of how the assessments are made when there are any changes and whether mitigation/compensation should be taken in nuclear safety and security areas when any results are derived after the assessment. Therefore, due to the lack of proper SSI management, there are possibilities that security measures may compromise safety functions and performance, and that safety requirements may increase threats. That is, the lack of relevant requirements, criteria, and guidance to ensure the substantial implementation of SSI makes it insufficient to ensure proper management of SSI. Therefore, it is necessary to establish and supplement subordinate statutes, technical standards and guidelines for implementing SSI-related content by referring to Table 1 proposed in RG 5.74.

On the other hand, regarding the safety assessment of nuclear power plants, the following problems can be found when reviewing large licensing process (construction permit, operating license) and replacing or changing facilities at nuclear power plants on operation. If an analog system is replaced with a digital system due to the aging of the operating power plant and discontinuation of existing facilities, safety should be reviewed and verified through "Application for Change Permit" or "Report of Changes in Minor Matters" in accordance with the *Nuclear Safety Act*. However, in terms of security, there is no requirement in the *Act on Measures for the Protection of Nuclear Facilities, etc. and Prevention of Radiation Disasters* that the facility replacement and design changes should be reviewed by regulatory body in advance, so it can not be considered that timely safety assessments and review of SSI related matters are being done.

In the case of large-scale licensing reviews such as Construction Permit and Operating License, the provisions of laws and regulations related to physical protection are not sufficient. Specifically, Section 13.6 (Physical Security) in the Standard Review Plan (NUREG-0800), a reference guide to the preparation of the Safety Analysis Report (PSAR, FSAR), is not specified in the *Act on Measures for the Protection of Nuclear Facilities, etc. and Prevention of Radiation Disasters*. However, the *Enforcement Decree of the Act on Measures for the Protection of Nuclear Facilities, etc. and Prevention of Radiation Disasters* stipulates that an application for approval of physical protection facilities, operating systems, physical protection regulations, emergency plans, and information system security regulations should be submitted by not later than five months before its commencing the use of the relevant nuclear facilities, etc. This cannot be said that SSI management of physical protection facilities, including cyber security, is timely done during the construction permit and/or operating license review process. Therefore, to improve these problems, it is necessary to stipulate that the safety analysis method should include Section 13.6 (Physical Security) in Chapter 13 of the Safety Analysis Report and identify and evaluate safety, security and SSI issues in the licensing review stage.

Regarding the SSI issues in the design of safety-grade digital instrumentation and control systems, to raise reliability of the software, excluding common cause failures, the safety of software system is reviewed and verified at each stage of the software development (requirements, designs, implementations, tests) in the nuclear safety field as shown in Fig.1.

According to regulatory requirements and guidelines related to safety evaluation of digital instrumentation and control systems, cyber security evaluation is also required in the nuclear security field according to the development stage of the nuclear safety sector. However, in the field of cyber security, due to the lack of related laws and regulations as mentioned above, the verification and evaluation activities of cyber security assessment, which should be prepared at each stage of software development, are not carried out properly. In case of conflict between software safety analysis and cyber security evaluations, insufficient cross-check of SSI between two regulatory expert organizations is a problem. Therefore, it is necessary to establish a cooperative framework between the two regulatory expert organizations along with the improvement of SSI management.

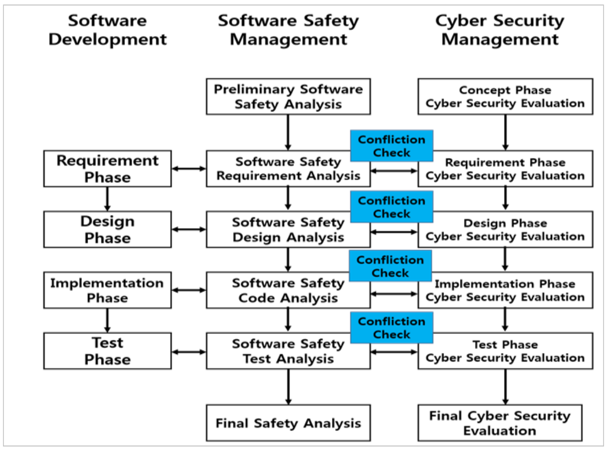
Software Development
Software Safety Management
Cyber Security Management
Preliminary Software Safety Analysis
Concept Phase Cyber Security Evaluation
Confliction Check
Requirement Phase
Software Safety Requirement Analysis
Requirement Phase Cyber Security Evaluation
Confliction Check
Design Phase
Software Safety Design Analysis
Design Phase Cyber Security Evaluation
Confliction Check
Implementation Phase
Software Safety Code Analysis
Implementation Phase Cyber Security Evaluation
Confliction Check
Test Phase
Software Safety Test Analysis
Test Phase Cyber Security Evaluation
Final Safety Analysis
Final Cyber Security Evaluation

Fig 1. SSI activities during the software development phase of the digital instrumentation and control system

Regarding the safety regulatory inspection of the nuclear safety-security interface, regular inspections of plant operators are conducted by each facility and item during the overhaul maintenance period of the plant. On the other hand, the nuclear security inspections of physical protection (including cyber security) consist of regular inspections (bi-annual) and special inspections under the *Act on Measures for the Protection of Nuclear Facilities, etc. and Prevention of Radiation Disasters*. However, safety-security interface activities, such as mutual inspection of nuclear safety and security interface or the sharing of results of each inspection with each other are not sufficient. Therefore, it is necessary to make efforts to conduct joint regulatory inspection in terms of SSI.

4. Conclusions

Without consideration, integration, and management of safety and security issues together in the design and operation of nuclear power plants, unintended consequences causing degradation of safety and/or security conditions are likely to happen. Therefore, the development of frameworks and mechanisms to promote a robust safety-security interface is critical in today's regulatory environment.

Integrated safety-security interface management is important to reduce conflicts between nuclear safety and security and to achieve a common goal of nuclear safety regulation. Therefore, it is necessary to establish a cooperative framework between regulatory expert organizations, along with supplement and improvement of related laws, regulations, and guidelines to improve the problem of managing nuclear safety-security interface.

REFERENCES

[1] 10 CFR 73.58, “Safety/Security Interface Requirements for Nuclear Power Plants.”

[2] 10 CFR 73.54, “Protection of Digital Computer and Communication Systems and Networks.”

[3] USNRC Reg. Guide 5.74(Rev.1), “Managing the Safety/Security Interface.”

[4] USNRC Reg. Guide 1.152, “Criteria for use of Computer in Safety Systems of Nuclear Power Plants.”

[5] USNRC Reg. Guide 5.71, “Cyber Security Programs for Nuclear Facilities.”

[6] USNRC Reg. Guide 1.173, “Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of NPPs.”

[7] NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for NPPs.”

[8] USNRC, Information Notice 2005-33: “Managing the Safety/Security Interface”

[9] U.S. Nuclear Regulatory Commission(NRC) Safety and Security – Policy and Oversight (IAEA-CN-254-258)

[10] U.S. Nuclear Regulatory Commission (NRC),“USNRC Efforts to Improve the Safety-Security Interface.”

[11] Min Baek, Sunghun Oh, “A Study on the Management of Nuclear Safety-Security Interface”, Transactions of the KNS Spring Meeting, 2020.7

[12] Nuclear Safety Act and its Enforcement Decree

[13] The Act on Measures for the Protection of Nuclear Facilities, etc. and Prevention of Radiation Disasters and its Enforcement Decree

[14] Guidelines for Safety Review of Light-water reactor-type Nuclear Power Plants (6th Edition, Revised) (KINS/GE-N001)