A Study on the Introduction of ITAAC (Inspection, Test, Analyses, Acceptance Criteria) in the Cybersecurity for Nuclear Power Plants

Song Lee*, Poe il Park, Kookheui Kwon
[a]*Korea Institute of Nuclear Nonproliferation and Control (KINAC), 1418 Yuseong-daero, Yuseong-gu, Daejeon 34101*
**Corresponding author: sssong@kinac.re.kr*

***Keywords:* Cybersecurity, Physical security, Combined License (COL), ITAAC**

1. Introduction

The licensing of nuclear power plants in the Republic of Korea currently follows the United States (U.S.) regulatory framework outlined in title 10 of the Code of Federal Regulations (10CFR) Part50. This framework divides the licensing process into two stages: construction permit and operating license. In the U.S., both 10CFR Part50 and 10CFR Part52 are used concurrently, with 10CFR Part52 introducing a Combined License (COL) system.

In the aspect of addressing climate change, the expansion of nuclear power generation, as a zero carbon energy source, is considered one of the most realistic alternatives for achieving carbon neutrality by 2050. Consequently, the development of Small Modular Reactor (SMR) is accelerating. As a result, the demand for nuclear regulation is expected to increase. To ensure prompt licensing and regulatory efficiency, the Republic of Korea should adopt the COL system based on 10CFR Part52. Under 10CFR Part52, the licensing procedures include an Early Site Permit (ESP), Standard Design Certification (SDC), and Combined License (COL).

When a licensee applies for Design Certification (DC), the Inspection, Test, Analyses, Acceptance Criteria (ITAAC) is submitted according to 10CFR Part52. Similarly, a ITAAC is submitted when applying for a COL. Additionally, COL applicants must submit physical security ITAAC for physical security systems. However, Nuclear Regulatory Commission (NRC) regulations do not specifically address ITAAC related to cybersecurity.

However, cybersecurity ITAAC is necessary to verify the effectiveness and reliability of cybersecurity control, address vulnerabilities, and continuously improve the security posture. This study proposes the introduction of Cybersecurity ITAAC, referred to as CS-ITAAC.

2. ITAAC Review

This section describes reviewing the current ITAAC system. According to NRC's DC standard outlined in 10CFR Part 52, ITAAC must be included in the DC application for the approval of the DC. The purpose of ITAAC is to verify that the certificated design and the performance and status of constructed reactor power plant are in alignment. ITAAC also severs to access whether the plant can operate in accordance with regulatory requirements and meet the standards set by the licensee.

Since DC and COL must be issued before construction of nuclear power plants, the completion status cannot be verified during the DC and COL audit stages. Consequently, the license is required to submit ITAAC. During construction, the licensee is responsible for performing all inspections, tests, analyses to ensure that the specified acceptance criteria are met. Subsequently, NRC inspectors will perform inspections based upon inspection manual chapter 2503 "Construction inspection program: inspection of ITAAC related work."

When a licensee follows the COL system of 10CFR Part52, a Design Control Document (DCD) is submitted when applying for design certification. DCD is divided into Tier 1 and Tier 2.

2.1 Tier1 ITAAC

Tier1 consists of (1) Definitions and General provisions (introduction), (2) Design Descriptions, (3) ITAAC, and (4) Site Parameters, etc. These information contains information, which allows reviewers to determine the suitability of design information and physically measurable data. Tier1 ITAAC includes design commitment, and safety-related verification activities such as inspection, test, analysis, and acceptance criteria.

Table1. Tier1 –Example of Emergency Cooling System (ECS) ITAAC [1].

Design Commitment	Inspection, Tests, Analyses	Acceptance Criteria
The ECS safety related accumulators provide a design usable water volume for emergency core reflood.	An inspection will be performed of the as built safety related accumulators.	The usable water volume of each ECS safety related accumulator is greater that or equal to 900 gallons.

2.2 Tier2 ITAAC

Tier2 consists of (1) A Final Safety Evaluation Report (FSAR), (2) An ITAAC, which was added a discussion to meet ITAAC standards, (3) A COL information item, (4) An Emergency Operating Guide (EOG). Also, Tier2 information includes more detailed information than recorded in Tier1. Tier2 ITAAC adds discussion of ITAAC implementation in the existing Tier1 ITAAC.

Table.2 Tier2 –Example of Emergency Cooling System (ECS) ITAAC [2].

Design Commitment	Inspection, Tests, Analyses	Acceptance Criteria	Discussion of Implementation
The ECS safety related accumulators provide a design usable water volume for emergency core reflood.	An inspection will be performed of the as built safety related accumulators.	The usable water volume of each ECS safety related accumulators is greater than or equal to 900 gallons.	Discusses that the ECS accumulators provide a usable volume for the safety related function of emergency core. An ITAAC inspection is performed to verify that the usable water volume of each ECS safety related accumulator in Tier1 is greater than or equal to 900 gallons.

2.3 Physical Security ITAAC; PS-ITAAC

To construct the nuclear power plants, licensees will submit many types of ITAACs. Security part ITAAC must be also submitted from licensees to receive the COL license. However, licensees are only considering the physical security of ITAAC in the security part.

PS-ITAAC means ITAAC related to physical security systems. The review of PS-ITAAC is conducted by NRC based on NUREG-0800 Standard Review Plan (SRP) 14.3 “Physical Security Hardware ITAAC”. Table 3 provides a list of physical security systems by the PS-ITAAC standard table in Appendix A of SPR 14.3. And the corresponding PS-ITAAC example is described well as shown in Table 4, but NRC regulations do not prescribe ITAAC for systems requiring cybersecurity.

Table 3. List of physical security systems

NO.	Physical Security Systems
1	Vital Areas and Vital Area Barriers
2	Protected Area Barriers
3	Isolation zones
4	Protected Area Perimeter Intrusion Detection and Assessment Systems
5	Illumination systems
6	Bullet Resisting Barriers
7	Vehicle Control Measures systems
8	Personnel, Vehicle, and Material Access-Control Portals and Search Equipment
9	Picture Badge Identification Systems
10	Access Control of Vital Areas
11	Alarm Stations
12	Secondary Power Supplies for Alarm-Annunciation and Communication Equipment
13	Console Displays and Alarms for Intrusion Detection Systems
14	Intrusion Detection systems’ recording Equipment
15	Emergency Exits from the Protected Area and Vital Areas
16	Communication systems

Table 4. Example of PS-ITAAC (Vital Equipment)

Design Commitment	Inspection, Tests, Analyses	Acceptance Criteria
Vital equipment will be located only within a vital area.	All vital equipment will be inspected to verify it is located within vital area.	All vital equipment is located only within a vital area.

2.4 Proposal of cybersecurity ITAAC; CS-ITAAC

Nuclear cybersecurity is the security of the computer and information systems of nuclear facilities about electronic infringement. [3] Additionally, cybersecurity prevents the computer and information systems of nuclear facilities from being adversely affected by cyberattacks that can cause unauthorized access and sabotage of nuclear facilities. This could be achieved by maintaining the confidentiality, integrity, and availability of system data that may adversely affect the safety, security, and emergency preparedness (SSEP) functions of a nuclear facility. [3]

Critical Digital Asset (CDA) is defined through the regulatory standards (KINAC/RS-015) of the Korea Institute of Nuclear Nonproliferation and Control. According to KINAC/RS-015, CDA is digital assets that could cause unauthorized removal or sabotage of nuclear facilities and computers, information systems that performs SSEP functions among critical systems or that affect SSEP functions.

Nuclear licensees shall verify information through physical walk down and electronic inspection to maintain cybersecurity and inspect the applied physical protection system for cybersecurity in nuclear power plant.

Table 4. Cybersecurity items for nuclear power plant

No.	Cyber security items
1	Logical and physical requirements for CDA and CS (Cybersecurity)
2	Communication requirement between Security Levels (4~2Level)
3	Implementation requirements of cybersecurity controls after security inspection
4	Network security facilities
5	Security monitoring facilities
6	Cyber-Intrusion Detection System (IDS)

The CS-ITAAC provided by the licensee serves to verify that the certified design and the performance and status of the nuclear cybersecurity systems are in alignment. By utilizing the acceptance criteria established according to regulatory requirements, the licensee can access the performance conditions of cybersecurity measures. Consequently, CS-ITAAC plays a crucial role in enhancing the effectiveness of cybersecurity for nuclear facilities. Table 4 above lists

the cybersecurity components for nuclear power plant that can be managed through CS-ITAAC.

Table 5. Example of the CDA items

NO.	CDA items
1	Fingerprint reader
2	Facial recognition device
3	Card reader
4	Plant visitor registration system

Table 6. Example of CS- ITAAC

System Commitment	Inspection, Tests, Analyses	Acceptance Criteria
System for monitoring the accessors and access control. And the access of the existing accessors record and control through an access control sever.	Review access control settings, authenticate access, and test access authorization.	The CDAs should appropriately grant user access permissions, accurately recognize the information of users with access permissions, and maintain user identification functionalities.

Table 5 provides example of CDA items used to monitor the identify of individuals accessing the facility and to manage personnel identification within the nuclear facility. Since these CDA items are responsible for controlling access authority, any malicious cyber activities targeting them could compromise the security functions of the nuclear facility, potentially resulting in sabotage. Thus, it is crucial to designate these digital assets as CDA, with illustrative examples detailed in Table 5.

To verify the setup requirements of the CDA items in Table 5, it is essential to thoroughly describe their role in system commitment section of Table 6. And descriptions related to cybersecurity inspections should be provide in the inspection and test analyses section. Furthermore, the criteria for evaluating the CDA through inspections, tests, and analyses should be outlined in the acceptance criteria section.

Therefore, Table 6 specifies that the system commitment includes the role of monitoring accessors' identities and controlling access. The inspection, Tests, analyses section should cover inspections related to access control settings and access authorization. Finally, the acceptance criteria for the CDA items should ensure that CDAs appropriately grant user access permissions, accurately recognize users with access rights, and maintain effective user identification functionalities.

3. Discussion and Conclusion

The main aspects of the combined license system in the U.S., such as ESP and SDC, have already been legislated in the Republic of Korea through similar mechanisms like Site Approval and Standard Design Certification. For research reactors, the legal framework for issuing combined construction permit and operational licenses was established under the Nuclear Safety Act and is actively used. Additionally, because APR1400 has already issued the SDC, it seems feasible to introduce the COL system.

However, the introduction of the COL system requires an ITAAC system to verify that the reactor has been completed by a certified design. According to 10CFR Part52, specific guidelines for the ITAAC of nuclear power plant devices, safety systems, and physical security systems are presented, but guidelines of ITAAC for cybersecurity are not presented.

As nuclear power plants gradually evolve, the increase in the number of cybersecurity system such as CDA and CS, Network security facilities, Security monitoring facilities in nuclear power plants is inevitable.

Additionally, the CS-ITTAC system can be used as a part of regulation activities, such as biannual regular inspections, or it could be utilized as one of the performance indicators in cybersecurity. CS-ITAAC is expected to establish a more reliable cybersecurity program for nuclear facilities by effectively meeting the compliance regulatory requirements. Furthermore, reviewing the CS-ITAAC during the COL stage makes it is possible to ensure the controls for the CDA in the D.C. stage. Also, by introducing the CS-ITAAC system, utilities can maintain the enhanced cybersecurity system. So, this study proposed the introduction of cybersecurity ITAAC for specific and efficient regulation activities to protect cybersecurity systems from cyberattacks.

REFERECES

[1] Kofons, Overview of Nuclear Regulatory Authorities in Major Foreign Countries, 2023

[2] J.E.Joo, J.S.Lee,.A Study on Regulatory Direction for Applying ITAAC to the KNGR, 1999

[3] In-kyung Kim, Ye-eun Byun, kook-heui Kwon, Analysis of the Application Method of Cyber Security Control to Develop Regulatory Requirement for Digital Assets in NPP, 2019

[4] NEI 15-02 Draft A of Revision, 2015

[5] NUREG-0800, 14.3 Inspection, tests. Analyses, and acceptance criteria