A Quantitative Evaluation Framework for Cyber Incident Response Exercises in Nuclear Facilities: Proposal, Scenario-Based Application, and Validation

Dong Jun Choi [a], Areum Ko [b] Jung Taek Seo [c*]
[a]*CPS Security Research Center, Gachon University, Seongnam-si, Korea*
[b] *Department of Information Security, Gachon University., Seongnam-si, Korea*
[c]*Department of Smart Security, Gachon University, Seongnam-si, Korea*

Keywords : nuclear facilities, Quantitative Evaluation, cyber incident response, Scenario-Based Application

1. Introduction

Nuclear facilities represent one of the most critical national infrastructures, where both safety and security must be ensured simultaneously. In recent years, cyberattacks targeting nuclear facilities have been reported both domestically and internationally. These attacks are regarded as serious threats because they can directly affect reactor control and safety systems, extending far beyond simple information leakage [1][2]. Accordingly, international organizations and regulatory authorities have consistently emphasized the need to strengthen cybersecurity and enhance response capabilities for nuclear facilities [3][4][5].

However, existing evaluation methods for cyber incident response exercises largely depend on qualitative judgments or focus only on verifying the fulfillment of individual components. Such approaches limit the ability to comprehensively and systematically validate operators' response capabilities in real-world attack scenarios, thereby reducing the effectiveness of training and preparedness. This highlights the necessity of an objective and reproducible quantitative evaluation framework that adequately reflects the unique characteristics of nuclear facilities.

To address these limitations, this study conducted scenario-based evaluations of cyber incident response exercises grounded in simulated cyberattack scenarios. Evaluation metrics, requirements, priorities, and performance objectives were applied to quantitatively assess diverse threat scenarios, and the proposed framework was empirically validated to confirm its practical applicability in operational environments.

The contributions of this paper are as follows. First, it proposes a quantitative evaluation approach that overcomes the limitations of existing qualitative methods for nuclear facilities. Second, it validates the proposed framework by applying it to real-world scenarios, thereby demonstrating its feasibility and practical utility. Third, it provides a foundation for developing future cyber incident response training programs and establishing regulatory standards.

The remainder of this paper is organized as follows. Section 2 reviews related studies and identifies the limitations of existing evaluation methodologies. Section 3 presents the proposed quantitative evaluation framework, including its evaluation metrics, requirements, priorities, and performance objectives. Section 4 describes the empirical results obtained by applying the framework to real-world threat scenarios. Finally, Section 5 discusses the significance and limitations of this study and outlines directions for future research..

2. Background and Related Works

2.1 Background

Cybersecurity in nuclear facilities must be managed from an integrated perspective of both safety and security, a principle that international regulatory authorities have consistently emphasized. The IAEA highlights that critical digital assets can affect essential functions such as safety, security, and emergency preparedness, and requires that these assets be protected against threat-based risks and quantitatively evaluated [5]. Similarly, the U.S. NRC, through 10 CFR 73.54, mandates that nuclear power plant operators establish a comprehensive cybersecurity program covering all critical digital systems and implement effective technical, administrative, and physical controls for all digital assets that may impact safety, security, and emergency preparedness functions [6].

In Korea, KINAC has issued the RS-015 regulation, which reflects international standards while also accounting for the operational characteristics of domestic nuclear facilities. In particular, it explicitly requires the identification of critical digital assets and the quantitative evaluation and management of their protection levels [7]. With the growing digitalization and automation of nuclear facilities, control systems such as ICS and SCADA have become primary targets of cyberattacks. Real-world cases such as the Stuxnet malware [8] demonstrate that similar threats can materialize in the nuclear sector. Therefore, advance preparation through cyber incident response exercises is essential, and quantitative evaluation of exercise performance levels is increasingly recognized as critical for enhancing cyber incident response capabilities.

2.2 Related Works

Several frameworks and studies have been proposed to evaluate cyber incident response capabilities.

ENISA's CSIRT Maturity Framework [9], MITRE's Cyber Resiliency Engineering Framework (CREF) [10], and CREST's Cyber Security Incident Response Maturity Assessment [11] provide systematic tools for assessment. However, these approaches mainly target general IT environments and do not adequately reflect the safety-critical characteristics of nuclear facilities.

Choi et al. [12] proposed a framework to evaluate the cyber incident response capabilities of nuclear facility operators through operation-based exercises. This study defined six response phases based on IAEA guidelines, established evaluation indicators for each phase, and validated the framework using simulator-based experiments. Nonetheless, a more comprehensive approach is still needed to integrate threat levels with performance objectives in a systematic and quantitative manner.

3. Proposed Quantitative Evaluation Framework

Section 3 describes, step by step, the procedures for applying the exercise-based capability evaluation methodology. The process consists of four stages:

- Classification of performance-objective types by cyber incident response phase
- Setting target levels for cyber incident response capabilities
- Assigning priority weights to performance objectives by type of cyberattack exercise scenario
- Deriving the overall exercise evaluation results

3.1 Classification of Performance Objective Types by Cyber Incident Response Phase

The framework proposed by Choi et al. [16] does not adequately reflect the objectives, purposes, types, and the phase-specific importance and characteristics of exercises. Therefore, this study introduces the concept of performance objectives into that framework and proposes an enhanced model that can be applied to diverse situations. The performance objectives were derived based on the requirements of NRC RG 5.71 and IAEA TDL-008, and their definitions are as follows.

- Rapidity: Considered in evaluating whether time-based objectives are met to prevent the spread of cyber threats and minimize damage.
- Consistency: Considered in assessing the degree of standardization of response quality across the organization, including whether processes are followed without deviation.
- Effectiveness: Considered in evaluating the outcomes and practical impact of response activities, such as preventing the adversary's objectives, protecting critical systems, and ensuring timely restoration of functions.
- Expertise: Considered in determining whether response personnel can take reliable actions based on technical knowledge, tool proficiency, and sound judgment.

The derived performance objectives are assigned to each cyber incident response phase according to its characteristics, thereby enabling clear diagnosis and systematic measurement of response capabilities. In the preparation phase, the focus is on verifying whether the exercise environment is properly established and whether operators possess the required expertise; thus, the performance objectives of consistency and expertise are assigned. In the Detection & Analysis phase, the goal is to promptly detect the occurrence of a cyber incident and accurately analyze relevant information to identify priority response targets; therefore, the performance objectives of timeliness and effectiveness are assigned. In the containment phase, the emphasis lies in isolating affected systems quickly and blocking the possibility of reinfection, which leads to the assignment of timeliness and effectiveness as performance objectives. The eradication phase requires identifying and removing the root cause of the incident while performing analysis and patching to prevent further attacks; as preventing recurrence and ensuring rapid and effective response are essential, the objectives of timeliness and effectiveness are assigned. In the recovery phase, the systems affected by the cyberattack must be restored to a normal state as quickly as possible while ensuring stability and functionality; hence, the objectives of timeliness and effectiveness are applied. Finally, the post-incident activity phase focuses on deriving improvements to prevent recurrence and reporting the outcomes to regulatory authorities, with evaluation centered on the standardized execution of procedures and operators' analytical and reporting capabilities; accordingly, the objectives of consistency and expertise are assigned.

Table 1: Performance Objectives

Cyber Incident Response Phase	Performance Objectives
Preparation	Consistency, Expertise
Detection & Analysis	Rapidity, Effectiveness
Containment	Rapidity, Effectiveness
Eradication	Rapidity, Effectiveness
Recovery	Rapidity, Effectiveness
Post Incident Activities	Consistency, Expertise

After assigning performance objectives to each cyber incident response phase, the evaluation requirements for each phase are examined, and the corresponding

performance objective types are allocated. This serves as a preparatory step for assigning priority weights to different types of cyber incident response training scenarios, and it is directly linked to Section 3.3. The evaluation requirements are based on the framework proposed by Choi et al. [16], and the mapping of performance objective types to each evaluation requirement is presented as follows. (ER, Evaluation Requirements)

Table 2 : Mapping of Evaluation Requirements and Performance Objectives by Cyber Incident Response Phase

Cyber Incident Response Phase Preparation	
ER	Prerequisite expertise of the cyber incident response team (P1, Expertise)
	Adequacy of cyber incident response training tools (P2, Expertise)
Cyber Incident Response Phase Detection & Analysis	
ER	Accuracy in identifying the root cause of a cyber incident (D1, Effectiveness)
	Level of understanding of the infection scope and propagation path (D2, Effectiveness)
	Accuracy in identifying potential impacts on critical systems (D3, Effectiveness)
	Adequacy of assessing the likelihood of a nuclear facility trip during a cyber incident (D4, Effectiveness)
	Rapidity of cyber incident detection (D5, Rapidity)
	Accuracy of cyber incident detection (D6, Effectiveness)
Cyber Incident Response Phase Containment	
ER	Adequacy of identifying containment strategies for the occurred cyber incident (C1, Effectiveness)
	Adequacy of blocking strategies for the spread and new infection paths of the cyber incident (C2, Effectiveness)
Cyber Incident Response Phase Eradication	
ER	Adequacy of evaluating the validity of information and evidence collection related to the cyber incident (E1, Effectiveness)
	Adequacy of root cause analysis of the cyber incident (E2, Effectiveness)
	Adequacy of applying system patches for cyber incident response (E3, Effectiveness)
	Rapidity in detecting additional cyberattacks (E4, Rapidity)
Cyber Incident Response Phase Recovery	
ER	Adequacy of recovery and reconfiguration of affected systems (R1, Effectiveness)
	Adequacy of verifying the normal operation of recovered systems (R2, Effectiveness)
Cyber Incident Response Phase Post Incident Activities	
ER	Specificity of reporting content for each cyber incident response procedure (I1, Consistency)
	Adequacy of evaluating the effectiveness of cyber incident response (I2, Consistency)
	Adequacy of reporting and disseminating the analyzed cyber incident (I3, Consistency)

In addition, as a concept included within the above evaluation requirements, 45 evaluation criteria have been defined to satisfy these requirements, as shown in Table.

Table 3 : Evaluation Criteria for Fulfilling Cyber Incident Response Requirements by Phase

Evaluation Criteria	Evaluation Criteria Identifier
Incident response history	P1.1
Completion status of cyber incident response training	P1.2
Implementation of corrective actions for deficiencies identified in past exercises	P1.3
Implementation status of IDS functionality	P2.1
Implementation status of alert functions for abnormal signs	P2.2
Accuracy of identifying the occurrence time of a cyber incident	D1.1
Accuracy of identifying characteristics of affected systems	D1.2
Accuracy of identifying the type of cyber incident	D1.3
Adequacy of identifying the nature and sophistication of the cyber incident	D1.4
Adequacy of identifying malware signatures with antivirus tools	D1.5
Accuracy of identifying physical interactions	D1.6
Accuracy of identifying attack vectors	D2.1
Accuracy of identifying information on attack hosts	D2.2
Accuracy of identifying impacts on systems and networks	D3.1
Accuracy of identifying data corruption	D3.2
Accuracy of identifying data exfiltration	D3.3
Accuracy of categorizing the severity of cyber incidents	D3.4

Accuracy of assessing the necessity of reactor shutdown during a cyber incident	D4.1
Rapidity of cyber incident detection	D5.1
Accuracy of identifying cyber incident–related events	D6.1
Adequacy of identifying potential resource damage and exfiltration	C1.1
Adequacy of identifying the time and resources required for containment measures	C1.2
Adequacy of identifying the duration and limitations of containment measures	C1.3
Success rate of system isolation	C2.1
Success rate of neutralizing new infection paths	C2.2
Diversity of data sources related to the cyber incident	E1.1
Adequacy of preserving cyber incident–related evidence	E1.2
Forensic validity of collected information and evidence	E1.3
Accuracy of identifying the origin of the cyber incident	E2.1
Adequacy of validating patch effectiveness	E3.1
Rapidity of patch application	E3.2
Rapidity of detecting additional cyber incident–related information	E4.1
Accuracy of prioritizing system recovery	R1.1
Adequacy of verifying the validity of backup systems used	R1.2
Adequacy of identifying proper operation of security solutions in recovered systems	R2.1
Adequacy of verifying the normal operation of recovered systems	R2.2
Adequacy of verifying the integrity of recovered systems	R2.3
Specificity of information about incident reporters	I1.1
Specificity of information about facilities related to the cyber incident	I1.2
Specificity of detailed information on the cyber incident	I1.3
Specificity of information regarding external support requests	I1.4
Adequacy of evaluating operators' performance in executing response tasks	I2.1
Adequacy of derived corrective measures	I2.2
Rapidity of reporting cyberattack information	I3.1
Adequacy of qualifications of reporting personnel	I3.2

Similarly, each evaluation criterion incorporates the content of practical performance indicators. In other words, evaluators can refer to the performance indicators to determine whether the evaluation criteria are satisfied, and subsequently use the criteria to assess whether the corresponding evaluation requirements have been fulfilled.

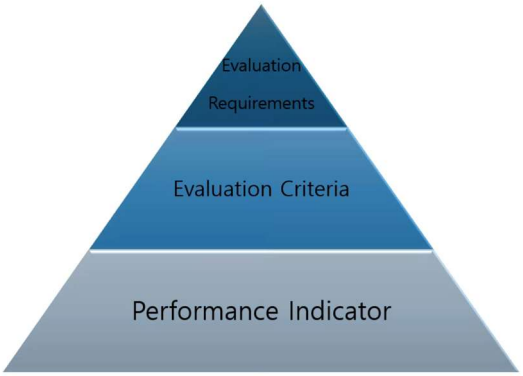

Fig. 1. Hierarchical Structure of Evaluation Requirements, Evaluation Criteria, and Performance Indicators

3.2 Setting Target Levels for Cyber Incident Response Capabilities

The target level of cyber incident response capability (R^i)is determined according to the threat level of the attack scenario (O^l). The threat level of each scenario is internally assigned based on factors such as its completeness and potential impact. Since the response capability target level must exceed the scenario's threat level, it is required to take a value equal to or greater than the assigned threat level. This stage represents the process of setting the minimum threshold for cyber incident response exercises.

(1) $O^l \leq R^i$

3.3 Assigning Priority Weights to Performance Objectives by Type of Training Cyberattack Scenario

The assignment of priority weights to performance objectives by type of training cyberattack scenario is proposed to address diverse attack situations. To this end, it is first necessary to classify the types of training cyberattack scenarios. In this study, cyberattack scenarios applicable to exercises are classified into two categories according to attack intent and potential impact.

The facility sabotage (destructive) threat scenario targets critical systems directly related to safe plant operation, such as the reactor protection system and safety instrumentation and control systems. This type

assumes an attack objective of causing severe accidents, such as the release of radiation or nuclear material.

The facility security and system malfunction threat scenario targets digital systems associated with physical protection functions, emergency operation systems for preventing radioactive release, systems supporting safety functions, and major digital systems related to power production. Although this type of attack does not directly cause the release of radiation or nuclear material, it assumes the objective of undermining plant security, reducing operational efficiency, or damaging equipment.

Among these, the facility sabotage (destructive) threat scenario requires rapid detection and appropriate judgment to contain the attack before the adversary achieves its objective. Accordingly, high priority is assigned to rapidity and effectiveness performance objectives in the Detection & Analysis and Containment phases. This enables focused evaluation of early response capabilities and technical decision-making skills during emergencies.

In the facility security and system malfunction threat scenario, it is crucial for operators to rapidly detect the attack, accurately analyze the abnormal situation, and effectively recover from it. Therefore, priority is given to rapidity and effectiveness in the Detection & Analysis, Eradication, and Recovery phases.

By assigning priority weights (W_i) to the response capability objectives (R^i)according to the importance of performance objectives in each phase, the baseline evaluation requirement value (R'_i) can be derived.

(2) $R'_i = R^i + W_i$

For example, let us assume that the type of training cyberattack scenario is a facility security and system malfunction threat scenario. Since this scenario assigns priority to rapidity and effectiveness in the Detection & Analysis, Eradication, and Recovery phases, additional priority weights can be applied to items D1~D6, E1~E4, and R1~R2. By assigning priority weights to the response capability objectives according to the scenario type, flexible evaluation across diverse scenarios becomes possible, enabling the assessment of response capabilities tailored to the intended attack objectives.

3.4 Evaluation Based on Cyber Incident Response Framework and Capability Assessment Techniques

The evaluator should conduct the assessment by comparing the phase-specific evaluation requirement baseline values (R'_i), which are established based on the evaluation requirements defined in the cyber incident response framework, with the performance scores (S_i^l) that represent the operators' actual capabilities measured during the exercise. The performance scores (S_i^l) are evaluated on a numerical scale ranging from 0 to 10. If the performance score (S_i^l) for a given evaluation requirement is greater than or equal to the corresponding baseline value (R'_i), the operator is considered to possess the level of capability required for the exercise and is assessed as Pass. Conversely, if the performance score (S_i^l) for a specific evaluation requirement is lower than the baseline value (R'_i), the operator is regarded as lacking the required capability for that evaluation requirement, and the corresponding area is identified as one requiring improvement and enhancement.

(3) $S_i^l \geq R'_i \ , \ 0 \leq S_i^l \leq 10$

3.5 Derivation of Overall Exercise Evaluation Results

The overall exercise evaluation results can be derived based on the performance evaluation scores (S_i^l) for each evaluation requirement and the phase-specific evaluation requirement criteria values (R'_i),as established in the cyber incident response framework. The overall evaluation result is calculated to confirm whether the operator meets the minimum competency level required for the exercise. This is determined by comparing the average of the phase-specific criteria values (R'_i) with the average of the performance evaluation scores (S_i^l). Specifically, if the average performance evaluation score (S_i^l) is greater than or equal to the average criteria value (R'_i), the operator is considered to have satisfied the minimum competency level required for the overall exercise.

(4) $\frac{1}{19}\sum_{i=p1}^{I3} S_i^l \geq \frac{1}{19}\sum_{i=p1}^{I3} R'_i$

4. Application of a Scenario-Based Quantitative Evaluation Framework

In this chapter, the proposed evaluation framework is applied to the sabotage threat scenario and the facility security and system malfunction threat scenario. The application of the framework requires a five-step procedure.

Table 4 : Procedural Steps for Applying the Evaluation Framework

Step	Description
1	Establishing response capability target levels
2	Assigning priority weights to performance objectives by type of training cyberattack scenario
3	Assigning and normalizing priority values for each phase
4	Comparing final evaluation reference values with performance scores
5	Deriving overall exercise capability evaluation results across all scenarios

First, the target level of response capability is established. This target must be set to be greater than or equal to the designated threat level, taking into account the risk and potential impact of the scenario. Second, performance objectives and their priority weights are assigned according to the type of training cyberattack scenario. The scenario type is identified, and the performance objectives for each response phase are determined. Third, priority weights are distributed across phases, and scores are normalized by dividing them by the number of evaluation criteria identifiers. Fourth, the final target evaluation values are compared with the measured performance scores obtained from the exercise, thereby identifying unmet evaluation requirements. Finally, the total of the evaluation values and the total of the performance scores are each divided by the number of evaluation identifiers, producing the final capability assessment result for the entire scenario-based cyber incident response exercise.

Based on this procedure, scenario-based evaluation is conducted. The first scenario is the Pressurizer Spray Valve Open case. In this scenario, the attacker manipulates the variable controlling the pressurizer (PRZ) spray valve flow, causing the spray valve to open. Such an attack reduces pressurizer pressure, which may prevent reactor cooling and lead to core meltdown with subsequent release of nuclear material. This constitutes a sabotage threat scenario for nuclear facilities. Accordingly, higher priority weights are assigned to the performance objectives of timeliness and effectiveness in the identification and detection phases, as well as in the containment phase.

The performance indicators for applying the cyber incident response capability evaluation framework to this scenario are organized as shown in Table.

Table 5: Evaluation Indicators and Performance Scores for the Pressurizer Spray Valve Open Scenario

Step	Indicator	Description	value
1	O^l	Target Threat Level	5
	R^i	Target Response Capability Level	5
2	W_i	Identification of Scenario-Specific Performance Objective Priorities	-
3	W_i	Timeliness in Identification and Detection Phase	0.3
		Effectiveness in Identification and Detection Phase	0.3
		Timeliness in Containment Phase	0.3
		Effectiveness in Containment Phase	0.3
	R'_i	Evaluation Criterion Values for D1, D2, D3, D4, D5, D6, C1, and C2 Requirements	5.3
	R'_i	Evaluation Criterion Values for Remaining Requirements	5
4	S_i^l	Performance Score for P1	10
		Performance Score for P2	10
		Performance Score for D1	8
		Performance Score for D2	5
		Performance Score for D3	5
		Performance Score for D4	10
		Performance Score for D5	0
		Performance Score for D6	10
		Performance Score for C1	7
		Performance Score for C2	10
		Performance Score for E1	7
		Performance Score for E2	10
		Performance Score for E3	10
		Performance Score for E4	10
		Performance Score for R1	10
		Performance Score for R2	10
		Performance Score for I1	7.5
		Performance Score for I2	5
		Performance Score for I3	10
5	$\frac{1}{19}\sum_{i=p1}^{I3} R'_i$	Average Criterion Value per Phase	5.13
	$\frac{1}{19}\sum_{i=p1}^{I3} S_i^l$	Average Performance Score	7.88

It was confirmed that, in the application of the scenario-based cyber incident response capability evaluation framework, the operator's response capability was insufficient in the indicators D2 (Accuracy in Identifying the Scope and Propagation Path of the Attack Infection), D3 (Accuracy in Identifying the Potential Impact on Essential Systems), and D5 (Timeliness of Cyber Incident Detection). In contrast, the overall average response capability level was 7.88, which exceeded the average criterion value of 5.13 per evaluation requirement, thereby demonstrating that the operator generally maintained an adequate level of response capability.

The second scenario is the Inadvertent Closing of a Steam Line Valve attack scenario. In this case, the attacker induces a single-point failure in the system controlling the steam line valve, resulting in the valve being closed. Closure of the steam line valve leads to a reduction in steam supplied from the main steam line, causing a decrease in turbine rotational speed. Consequently, the turbine protection system is activated, resulting in turbine trip and RX trip. This scenario is therefore classified as both a facility security and system failure threat scenario. Accordingly, higher priority weights are assigned to the performance objectives of Timeliness and Effectiveness in the Identification and Detection Phase, Timeliness and Effectiveness in the Eradication Phase, and Timeliness and Effectiveness in the Recovery Phase.

The performance indicators for applying the cyber incident response capability evaluation framework to this scenario are organized as shown in Table.

Table I: Performance Objectives.

Step	Indicator	Description	value
1	O^l	Target Threat Level	6
	R^i	Target Response Capability Level	6
2	W_i	Identification of Scenario-Specific Performance Objective Priorities	-
3	W_i	Timeliness in Identification and Detection Phase	0.3
		Effectiveness in Identification and Detection Phase	0.3
		Timeliness in Eradication Phase	0.3
		Effectiveness in Eradication Phase	0.3
		Timeliness in Recovery Phase	0.5
		Effectiveness in Recovery Phase	0.5
	R'_i	Evaluation Criterion Values for D1, D2, D3, D4, D5, D6, E1, E2, E3, and E4 Requirements	6.3
		Evaluation Criterion Values for R1 and R2 Requirements	6.5
	R'_i	Evaluation Criterion Values for Remaining Requirements	6
4	S_i^l	Performance Score for P1	10
		Performance Score for P2	10
		Performance Score for D1	10
		Performance Score for D2	10
		Performance Score for D3	5
		Performance Score for D4	10
		Performance Score for D5	0
		Performance Score for D6	10
		Performance Score for C1	7
		Performance Score for C2	10
		Performance Score for E1	7
		Performance Score for E2	10
		Performance Score for E3	10
		Performance Score for E4	10
		Performance Score for R1	10
		Performance Score for R2	0
		Performance Score for I1	7.5
		Performance Score for I2	5
		Performance Score for I3	0
5	$\frac{1}{19}\sum_{i=p1}^{I3} R'_i$	Average Criterion Value per Phase	6.21

	$\frac{1}{19}\sum_{i=p1}^{I3} S_i^l$	Average Performance Score	7.45

As a result of applying the scenario-based cyber incident response capability evaluation framework, it was confirmed that the operator's response capability was insufficient in the indicators D3 (Accuracy in Identifying the Potential Impact on Essential Systems), D5 (Timeliness of Cyber Incident Detection), R2 (Adequacy of Verification for the Normal Operation of Recovered Systems), I2 (Adequacy of Assessing the Effectiveness of Cyber Incident Response), and I3 (Adequacy of Reporting and Disseminating the Analyzed Cyber Incident). Nevertheless, the overall average response capability level was 7.45, which exceeded the average criterion value of 6.21 per evaluation requirement, thereby confirming that the operator generally maintained an adequate level of response capability.

5. Conclusion

This study proposed a quantitative evaluation framework that introduces phase-specific performance objectives and integrates scenario-based priority weighting with target capability levels in order to objectively assess the outcomes of cyber incident response exercises in nuclear facilities. Through this approach, the evaluation, which had previously relied on qualitative judgment, is transformed into a systematic management foundation that connects exercise design, execution, and improvement.

The application results for two representative scenarios are as follows. First, in the PRZ Spray Valve Open scenario, indicators D2, D3, and D5 were identified as vulnerable areas. Nevertheless, the average performance score of 7.88exceeded the average criterion value of 5.13, indicating that the overall response capability met the target level. Second, in the Steam Line Valve Closing scenario, indicators D3, D5, R2, I2, and I3 in the detection, recovery, and post-incident phases were identified as priority areas for improvement. However, the average performance score of 7.45 exceeded the average criterion value of 6.21, thereby confirming the validity of baseline capability. These findings suggest that the proposed framework provides practical decision-making evidence by presenting both the overall degree of capability fulfillment and phase- or scenario-specific weaknesses, thus supporting the prioritization of training objectives, allocation of resources, and specification of follow-up improvement tasks.

Furthermore, by differentiating priority weights according to scenario characteristics, response capabilities across the preparation, identification and detection, containment, eradication, recovery, and post-incident phases can be aligned in a performance-oriented manner. Unmet indicators can be directly translated into actionable improvement tasks such as procedural reinforcement, capability enhancement, additional training, and joint exercises across organizational units.

Limitations also exist. First, the setting of target capability levels and priority weights, which are based on scenario risk levels, involve expert judgment, thereby introducing the possibility of variability across institutions and sites. Second, the number of applied scenarios and system types was limited, requiring caution in generalization.

Accordingly, future research will focus on quantitatively assessing the impact and risk of scenarios and developing methods to derive priority weights quantitatively rather than relying on evaluator judgment. The proposed framework, by providing a consistent and integrated structure, ensures objectivity, reproducibility, and explainability in cyber incident response exercises for nuclear facilities. It is expected to contribute to the establishment of standardized quantitative evaluation and the development of sustainable capability improvement mechanisms in high-risk critical infrastructures.

ACKNOWLEDGMENT

This work was supported by the Nuclear Safety Research Program through the Korea Foundation of Nuclear Safety(KoFONS) using the financial resoruce granted by the Nuclear Safety and Security Commission(NSSC) of the Republic of Korea.(RS-2021-KN051410).

REFERENCES

[1] International Atomic Energy Agency (IAEA), Computer Security of Instrumentation and Control Systems at Nuclear Facilities, Nuclear Security Series No. 17, Vienna: IAEA, 2011.
[2] U.S. Nuclear Regulatory Commission (NRC), Cyber Security Programs for Nuclear Facilities (10 CFR 73.54), Washington D.C.: NRC, 2009.
[3] Korea Institute of Nuclear Nonproliferation and Control (KINAC), Regulatory Standard on Cybersecurity for Nuclear Facilities (KINAC/RS-015), Daejeon: KINAC, 2021.
[4] European Union Agency for Cybersecurity (ENISA), CSIRT Maturity Framework, ENISA, 2020.
[5] IAEA, Computer Security at Nuclear Facilities, Nuclear Security Series No. 17, International Atomic Energy Agency, Vienna, 2011.
[6] U.S. Nuclear Regulatory Commission, 10 CFR 73.54 Protection of digital computer and communication systems and networks, U.S. NRC, 2009.
[7] Korea Institute of Nuclear Nonproliferation and Control (KINAC), Regulation on Cybersecurity of Nuclear Facilities (RS-015), KINAC, 2016.
[8] S. Karnouskos, "Stuxnet Worm Impact on Industrial Cyber-Physical System Security," 37th Annual Conference of the IEEE Industrial Electronics Society, 2011.
[9] European Union Agency for Cybersecurity (ENISA). CSIRT Maturity Framework. ENISA, 2017.

[10] MITRE. Cyber Resiliency Engineering Framework (CREF). MITRE Technical Report, 2020.
[11] CREST. Cyber Security Incident Response Maturity Assessment. CREST, 2019.
[12] H. Choi, C. Park, J. Lee, S. Jeon, and J. Seo, "Framework for evaluating cyber incident response capabilities of nuclear facility operators through operation-based exercises," Nuclear Engineering and Technology, Vol. 57, No. 11, pp. 103772, 2025.