Classification Criteria for Performance Objectives in Cyber Incident Response Capability Evaluation at Nuclear Facilities

Areum Ko [a], Dong Jun Choi [b], Jung Taek Seo [c*]
[a]*Department of Information Security, Gachon University., Seongnam-si, Korea*
[b]*CPS Security Research Center, Gachon University, Seongnam-si, Korea*
[c]*Department of Smart Security, Gachon University, Seongnam-si, Korea*
[*]*Corresponding author: seojt@gachon.ac.kr*

***Keywords :** nuclear facilities, cyber incident response, performance objectives, response capability

1. Introduction

Operators of nuclear facilities must conduct regular response exercises to ensure their capability to detect and respond to cyber incidents that could affect Safety, Security, and Emergency Preparedness (SSEP) systems [1]. Regulatory authorities evaluate these exercises in accordance with relevant guidelines, such as KINAC/RS-011 [2,3]. However, these guidelines define each component of the exercise only at a high level, which limits their effectiveness in supporting systematic and objective assessments of response capabilities.

To address these limitations, Choi et al. [4] refined the cyber incident response process into six distinct phase and proposed phase-specific evaluation requirements, thereby establishing a foundation for exercise-based assessment frameworks. However, this approach is constrained by the assumption that all phases and situations can be evaluated using uniform criteria. In practice, the performance objectives required during incident response may vary depending on the circumstances. For instance, in the early detection and containment phases, rapidity may be critical, whereas in the post-incident investigation phase, expertise may be more essential. Therefore, it is necessary to map phase-specific evaluation requirements to corresponding performance objectives, enabling differentiated assessments and quantitative analyses tailored to each situation.

In this paper, we propose four performance objectives—rapidity, consistency, effectiveness, and expertise—for evaluating cyber incident response capabilities, and map them to the response phases defined by Choi et al. [4]. This approach provides a foundation for more systematic and quantitative assessments of nuclear facility operators' response capabilities. The contributions of this paper are as follows.

- We propose four performance objectives for cyber incident response in nuclear facilities.
- We map the proposed performance objectives to the phases of cyber incident response, thereby structuring the key competencies required at each phase.

The remainder of this paper is organized as follows. Section 2 reviews the classification criteria of evaluation indicators applied in critical infrastructures and introduces related works. Section 3 presents the proposed performance objectives and their mapping to response phases. Section 4 discusses the applicability and implications of the proposed framework. Finally, Section 5 provides the conclusion and outlines directions for future research.

2. Background and Related Works

Section 2 provides the relevant background and related works. First, it examines the classification criteria for cyber incident response capabilities applicable to critical infrastructures. It then explains the phase-specific structure of the cyber incident response framework proposed by Choi et al. [4].

2.1 Background

To quantitatively evaluate cyber incident response capabilities, it is essential to classify response activities into distinct phases and clearly define the required performance objectives for each phase. Previous studies have proposed various classification criteria to address this need.

NIST SP 800-61 categorizes the computer security incident response lifecycle into preparation, detection and analysis, containment, eradication and recovery, and post-incident activity, providing requirements for each phase [5]. Gartner evaluates the maturity of security programs using the Consistent, Adequate, Reasonable, and Effective (CARE) classification criteria [6]. Staves et al. [7] divided incident response and recovery in Industrial Control System (ICS) environments into four phases: Planning, Preparation, Mid-Incident, and Post-Incident. In addition, NIST CSF 2.0 classifies cybersecurity activities into Govern, Identify, Protect, Detect, Respond, and Recover [8], while BTIB introduced consistency, diversity, and rapidity as classification criteria [9].

Although these existing criteria have structured response frameworks and provided evaluation indicators, they are primarily focused on specific organizational contexts and therefore have limitations in fully reflecting the unique regulatory requirements and protection priorities of nuclear facilities.

2.2 Related Works

Rick Van der Kleij et al. [10] analyzed challenges at the organizational, team, individual, and instrumental levels, and proposed improvements to enhance the performance of Computer Security Incident Response Teams (CSIRTs) through situation awareness–based sensemaking.

Abdulaziz Gulay et al. [11] employed the Integrated Risk Management (IRM) approach to analyze the prioritization and interdependencies of cyber incidents and proposed effective response plans that take into account human and organizational factors.

Choi et al. [4] proposed a exercise-based framework to evaluate the cyber incident response capabilities of nuclear facility operators. This framework divides the response process into six phase—Preparation, Detection & Analysis, Containment, Eradication, Recovery, and Post-Incident—and specifies evaluation requirements for each phase. The framework refines the Mitigation phase defined by the International Atomic Energy Agency (IAEA) into Containment, Eradication, and Recovery, thereby enabling the establishment of tailored requirements aligned with the characteristics of each phase. The phase-specific requirements for cyber incident response are summarized in Table I.

Table I: Activities for each phase of cyber incident response cycle[4].

Phase	Description
Preparation	To conduct cyber incident Response Exercises for nuclear facilities, it is essential to evaluate the competency level of operators and ensure the readiness of the exercise environment.
Detection & Analysis	Rapidly detect cyber incidents and identify and analyze related information.
Containment	Rapid and secure isolation of affected systems and suppression of cyberattack reinfection rates.
Eradication	Perform forensic analysis and patching for Cyber Incidents and rapidly detect any additional incidents.
Recovery	Take rapid and secure recovery actions for affected systems.
Post-incident	Identify improvements to prevent the recurrence of Cyber Incidents and similar events and report them to regulatory authorities

This study maps performance objectives to each of the six phases presented in Table I. Through this mapping, it identifies the core competencies required at each phase of the actual cyber incident response process and establishes a foundation for systematic and quantitative evaluation.

3. Performance Objectives for Cyber Incident Response in Nuclear Facilities

Section 3 proposes classification criteria for performance objectives tailored to nuclear facilities, addressing the limitations of previous studies. The proposed performance objectives consist of four elements: Rapidity, Consistency, Effectiveness, and Expertise. These objectives are defined based on the requirements outlined in NRC RG 5.71 [1] and IAEA TDL-008 [12], thereby ensuring alignment with international standards. The definitions of each performance objective are presented in Table II.

Table II: Performance Objectives.

Performance Objectives	Description
Rapidity [1]	The ability to execute each response phase without delay and to complete necessary actions in a timely manner.
Consistency [1]	The ability to perform responses at the same level under identical conditions, regardless of incident type or personnel, based on established procedures and manuals.
Effectiveness [1]	The extent to which incident response activities contribute to blocking the adversary's intent or objectives, minimizing the impact of the incident, and ensuring functional recovery.
Expertise [12]	The technical competence and situational judgment to accurately and proficiently employ appropriate tools and procedures during incident response.

The derived performance objectives can be applied as key evaluation criteria in practical assessments, 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.

Furthermore, the performance objectives can be mapped to the six phases of cyber incident response, as shown in Table III. This mapping enables systematic and quantitative evaluation of the core competencies required at each phase.

Table III: Performance Objectives.

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

- **Rapidity and Effectiveness** are the primary performance objectives emphasized in the phases from Detection & Analysis to Recovery, as these phases demand immediate actions and outcome-oriented performance to prevent the spread of cyber threats and ensure rapid restoration of system functionality.
- **Consistency and Expertise,** on the other hand, are the performance objectives that characterize the Preparation and Post-Incident phases, since these phases focus less on real-time actions and more on the establishment of standardized procedures and the proficiency of responders.

In this manner, each performance objective can be categorized according to the corresponding response phase, and the evaluation requirements of each phase can further be classified based on the associated performance objectives. For example, within the Detection & Analysis phase, time-based evaluation requirements such as “Timely detection of the cyber incident” [4] can be classified under the Rapidity performance objective. Similarly, requirements such as “Identification of attack infection boundary and propagation path” [4], which aim to block the attacker’s intent or prevent the spread of impact, can be classified under the Effectiveness performance objective. Such mappings enable the structuring of phase-specific evaluation requirements in connection with performance objectives, thereby providing a practical foundation for quantitative and objective assessment of nuclear facility operators’ cyber incident response capabilities.

4. Discussion

The performance objective classification criteria proposed in this paper provide a foundation for quantitatively evaluating cyber incident response capabilities by reflecting the unique characteristics of nuclear facilities. The four performance objectives—Rapidity, Consistency, Effectiveness, and Expertise—address the qualitative limitations of existing evaluation methods that rely heavily on subjective judgment, and instead allow for the clear differentiation of core competencies required in each response phase. This enables the use of quantitative indicators such as detection time, containment success rate, and procedural compliance rate, while also facilitating the identification of priority evaluation areas for each phase.

In particular, when integrated into exercise-based assessments, the performance objectives can be prioritized according to the type and purpose of the exercise as well as the significance and characteristics of each response phase. Evaluators may assign differential weights to evaluation requirements based on the priority of the corresponding performance objectives, score them accordingly, and aggregate the results to derive a final quantitative score. This approach transforms conventional qualitative assessments into systematic, data-driven analyses, thereby ensuring objectivity and comparability of evaluation outcomes, and ultimately enabling a quantitative and structured diagnosis of exercise results.

In addition, the proposed performance objectives can contribute to the standardization of evaluation requirements by regulatory authorities. Since each objective is defined based on international guidelines such as NRC RG 5.71 and IAEA TDL-008, they can be utilized to design domestic evaluation frameworks in alignment with international standards. Moreover, the four performance objectives—Rapidity, Consistency, Effectiveness, and Expertise—provide a foundational structure that can be universally applied. Accordingly, regulatory authorities can use this framework to establish a minimum set of common requirements and to compare and analyze evaluation results in a consistent manner. This, in turn, is expected to enhance the objectivity and reliability of exercise-based assessments.

While this study presents a foundational framework for the quantification of evaluation systems through performance objectives, it does not propose specific methodologies for quantitative measurement. For instance, Rapidity can be measured using indicators such as detection time or recovery time; however, further research is required to determine how these values should be standardized and how threshold levels should be established.

5. Conclusion and Future Work

This paper proposed classification criteria for performance objectives to quantitatively evaluate cyber incident response capabilities in nuclear facilities. The four performance objectives—Rapidity, Consistency, Effectiveness, and Expertise—address the qualitative limitations of conventional evaluation methods and enable the identification of core competencies required in each response phase. This allows for the determination of priority evaluation areas and the execution of

quantitative assessments based on those areas, which constitutes a key contribution of this study. Furthermore, the proposed performance objectives, by ensuring alignment with international guidelines, can support regulatory authorities in establishing standardized evaluation requirements, while providing operators with a systematic and objective tool for capability assessment. Future research will focus on applying actual exercise cases to develop concrete quantitative metrics grounded in the proposed performance objectives.

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] U.S. Nuclear Regulatory Research, Regulatory Guide 5.71(Cyber Security Programs for Nuclear Facilities), 2010.
[2] Korea Institute of Nuclear Nonproliferation and Control. KINAC/RS-011: Cyber Security Response Training for Nuclear Facilities, 2024.
[3] Republic of Korea, Regulation on Physical Protection Education and Training, Art. 13, “Training,” 2021.
[4] Choi, Heewon Aneka, et al. Framework for Evaluating Cyber Incident Response Capabilities of Nuclear Facility Operators through Operation-Based Exercises. Nuclear Engineering and Technology, 2025.
[5] NIST, Computer Security Incident Handling Guide. NIST SP 800-61(Rev. 2). Gaithersburg, MD, 2012.
[6] Gartner, 4 Metrics That Prove Your Cybersecurity Program Works, https://www.gartner.com/en/articles/4-metrics-that-prove-your-cybersecurity-program-works#:~:text=Effectiveness %20metrics
[7] Staves, Alexander, et al. A cyber incident response and recovery framework to support operators of industrial control systems. International Journal of Critical Infrastructure Protection, 2022.
[8] Pascoe, C. E., The NIST Cybersecurity Framework(CSF) 2.0. National Institute of Standards and Technology, 2024.
[9] BTIB, Cybersecurity Incident Response Manual 2024, 2024.
[10] Rick Van der Kleij, Geert Kleinhuis, Heather Young, Computer security incident response team effectiveness: A needs assessment, Front. Psychol. 8 2017.
[11] Abdulaziz Gulay, Leandros Maglaras, Alignment of Cybersecurity Incident Prioritisation with Incident Response Management Maturity Capabilities, Edinburgh Napier University, Edinburgh, UK, 2024.
[12] IAEA, Preparation, Conduct and Evaluation of Exercises to Test Security Contingency Plans at Nuclear Facilities, 2018.