An Integrated Cybersecurity Maturity Assessment Framework for Nuclear Facilities

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

Keywords : Cyber Security, Nuclear Facility, Maturity Model, Security Assessment

1. Introduction

Cyberattacks on industrial control systems (ICS) are increasing, and their methods are becoming more sophisticated [1]. The SANS State of ICS/OT Security 2025 report [2] found that 22 percent of surveyed experts had experienced a security incident in an ICS or OT environment within one year. Nuclear facilities are also increasingly exposed to such attacks as digital technologies are introduced into their I&C systems [3]. A cyber incident at a nuclear facility can go beyond information leakage or service disruption. Through damage to or malfunction of I&C systems, it can impair Safety, Security, and Emergency Preparedness (SSEP) functions, which can lead to consequences as severe as radiological impacts.

Such attacks can cause loss of life beyond economic and physical damage, so a security review of an organization's posture and capability is needed before an attack occurs. Security maturity models are widely used for this purpose. They provide the level of performance for each security function, which enables an organization to systematically diagnose its capability and to derive directions for improving deficient areas [4]. However, most existing models are designed for general information technology environments or for specific industrial sectors, so they do not sufficiently reflect the characteristics that are unique to nuclear facilities, which must protect safety as the highest priority [5]. In addition, because each model differs in its target, its domains, and its level scheme, the results of different models are difficult to interpret together even when the models are used side by side [6]. We therefore derive requirements from existing security maturity models and from nuclear facility regulations and guidelines, and we reconstruct them into maturity level requirements for each security function. The contributions of this paper are as follows.

- We present the security characteristics that are specific to nuclear facilities, and we show that the proposed model reflects them.
- We jointly derive and integrate, from regulatory documents, the safety and security linkage and the regulatory requirements of nuclear facilities that general maturity models cannot capture on their own.
- By converting results that were expressed in different domains and level schemes into six functions, we enable the results of multiple frameworks to be compared and interpreted under a consistent criterion.

The paper is organized as follows. Section 2 reviews existing maturity models and nuclear facility regulatory requirements. Section 3 analyzes the security characteristics that are unique to nuclear facilities. Section 4 describes the functions, the levels, and the derivation and mapping methods of the proposed model. Section 5 applies the model to RG 5.71, and Section 6 concludes the paper and discusses future work.

2. Background

This section analyzes the structure and the level scheme of each security maturity model, and it identifies the characteristics of nuclear facilities from regulatory documents.

2.1 Existing Security Maturity Models

A cybersecurity maturity model assesses the level at which an organization's security activities are established and operated. Existing models differ in their target and in their level scheme, but they commonly distinguish levels according to whether activities are performed, whether they are documented, whether they are repeated, whether they are managed at the organizational level, and whether they are continuously improved. Each model also classifies security activities into domains or categories and places individual requirements underneath them. This section reviews the structure and the level scheme of CS-CMM, C2M2, C2M2-Nuclear, CMMC, ENISA CSIRT Capabilities, and NIST CSF 2.0, which are applicable to nuclear facility security assessment.

The Cyber Security Capability Maturity Model (CS-CMM) [7] is included in the minimum cybersecurity standards of the New Zealand National Cyber Security Centre (NCSC). It comprises ten security standard domains, such as Risk Management, Assets and their Importance, Patching, and Multifactor Authentication. Each domain has four maturity levels, which are Informal, Planned and tracked, Standardised, and Quantitatively controlled.

The Cybersecurity Capability Maturity Model (C2M2) [8] was presented by the U.S. Department of Energy (DOE) to assess security capability in IT and OT environments. It comprises ten domains, such as Asset, Threat, and Situation. Each domain is subdivided

into Objectives and Practices, to which a Maturity Indicator Level (MIL) from 0 to 3 is assigned. C2M2-Nuclear [9] extends C2M2 to the nuclear sector. It adds the PHYSICAL and EXTENT domains, resulting in twelve domains in total, and its level scheme is identical to that of C2M2.

The Cybersecurity Maturity Model Certification (CMMC) [10] was developed to verify that companies in the Defense Industrial Base (DIB) implement appropriate cybersecurity practices. It presents requirements across fourteen domains, such as Access Control, Configuration Management, and Security Assessment. Its three certification levels, which are Foundational, Advanced, and Expert, certify the protection of Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

The ENISA CSIRT Capabilities framework [11] assesses the incident management maturity of national Computer Security Incident Response Teams. It is based on the Security Incident Management Maturity Model (SIM3) [12] and presents parameters for four categories, which are Organisation, Human, Tools, and Processes. Each parameter is assessed on a fivelevel scale from 0 to 4.

NIST CSF 2.0 [13] provides guidance that helps organizations of all sizes and sectors manage and reduce cybersecurity risk. It organizes cybersecurity outcomes at a high level through six core functions, which are Govern, Identify, Protect, Detect, Respond, and Recover. It also defines four tiers, which are Partial, RiskInformed, Repeatable, and Adaptive, and these tiers express the level of an organization's cybersecurity risk governance and management activities.

2.2 Nuclear Facility Regulations and Guidelines

Unlike general IT and OT environments, nuclear facilities must meet separate regulatory requirements in order to protect safety and security related functions. These requirements are unique to nuclear facilities and are not addressed by general maturity models. This section reviews NRC RG 5.71, which provides guidance for cybersecurity programs, and IAEA TDL-005, which presents cyber incident response procedures in stages.

IAEA TDL-005 [14] provides key elements and guidance for developing and implementing a comprehensive response framework for cyber incidents at nuclear facilities. Based on the incident response life cycle, it presents nuclear facility specific procedures for preparation, detection and analysis, mitigation(containment, eradication, recovery), postincident activity, and reporting. For each procedure, it also specifies the tasks of operators, regulatory bodies, and technical support organizations.

The Nuclear Regulatory Commission (NRC) published Regulatory Guide 5.71, titled Cyber Security Programs for Nuclear Power Reactors [15]. This guide presents requirements for protecting safety systems, systems that are essential to safety, security functions, and emergency preparedness facilities.

3. Analysis of the Nuclear Facility Environment

In nuclear facilities, I&C systems support SSEP functions. These systems were once operated in an analog manner, but they have adopted digital technologies in order to process large amounts of process data and to improve operational efficiency. As SSEP functions came to depend on digital assets, their exposure to cyberattacks also increased. A cyber incident can impair SSEP functions through damage to or malfunction of I&C systems. Such impairment can lead to radiological sabotage, unauthorized access to sensitive nuclear information, or unauthorized removal of nuclear material. The cybersecurity of nuclear facilities is therefore essential for protecting both nuclear security and nuclear safety.

General ICS environments consider safety and reliability in addition to confidentiality, integrity, and availability, and they often prioritize availability in order to maintain the continuity of processes. In nuclear facilities, however, a cyber incident can lead to radiological consequences through the loss or degradation of safety functions, so safety is regarded as the foremost protection target. When an incident occurs, priority is given not only to blocking the spread of the attack but also to preventing progression to an accident state and to keeping the plant in a safe state. Such measures may include procedures for preserving safety functions, such as the shutdown of safety systems.

Nuclear facility security thus has the distinctive requirement of protecting digital assets that are linked to SSEP functions and of maintaining safety and security functions when an incident occurs. Existing general maturity models are designed for IT environments or for specific industrial sectors, so they do not sufficiently reflect these safety centered characteristics and nuclear security requirements. Because the models also differ in their domains and level schemes, their results are difficult to interpret in an integrated manner. Assessing the security level of a nuclear facility therefore requires a maturity model that jointly reflects general models and regulatory requirements within a consistent function and level scheme.

4. Proposed Model

We propose a model that assesses the cybersecurity maturity of nuclear facilities by integrating existing maturity models and regulatory requirements. The model reconstructs the differing domains and level schemes into security functions and a common maturity scheme, and it maps the derived requirements to the level of each function. Through the four levels Baseline, Developing, Managed, and Optimized, the model determines the security level of a facility by function.

4.1 Function Definition of the Maturity Model

We introduce security functions as the classification axis of the model. Because existing models use different domain schemes, such as asset management, access control, and risk management, their requirements are difficult to compare or integrate directly. A comprehensive function scheme is therefore needed so that various models and regulatory requirements can be reclassified under a consistent criterion.

We adopt the six functions of NIST CSF 2.0, which are Govern, Identify, Protect, Detect, Respond, and Recover, as the common classification scheme. Because CSF 2.0 spans the full range of activities from governance to incident recovery and applies to both IT and OT environments, it is suitable for reclassifying existing models and regulatory requirements into consistent functions. The definition of each function is given in Table 1 with reference to CSF 2.0.

Table I: Function Definitions

Function	Definition
Govern	Establishes and manages the organization's cybersecurity strategy, policies, roles and responsibilities, and risk management scheme.
Identify	Identifies the organization's assets, systems, supply chain, and risks in order to prioritize protection, and identifies improvements after incident response.
Protect	Applies access control, training, data security, and infrastructure protection to the identified assets and systems.
Detect	Promptly discovers and analyzes possible cybersecurity attacks or signs of compromise.
Respond	Contains the impact of a detected cybersecurity incident and performs analysis, mitigation, reporting, and communication.
Recover	Restores the assets and operations affected by an incident to a normal state and communicates the progress.

4.2 Level Definition of the Maturity Model

A maturity level distinguishes, in stages, how well security activities are established and advanced. Existing models were found to commonly distinguish levels according to performance, documentation, repetition, organization level management and measurement, and feedback and continuous improvement. On this basis, we define four levels, which are Baseline, Developing, Managed, and Optimized. The definition and basis of each level are given below and in Table 2.

Table II: Maturity Level Definitions and Basis

Level	Level Definition	Basis for Level Derivation
Baseline	The minimum operational level at which the essential security activities for nuclear facility security are performed	CS-CMM Level 2 C2M2/C2M2-Nuclear MIL1 ENISA CSIRT Level 1 CMMC Level 1
Developing	The level at which basic security activities are established and operated based on documented procedures and resources	C2M2/C2M2-Nuclear MIL2 ENISA CSIRT Level 2 NIST CSF 2.0 Tier 2
Managed	The level at which security activities are repeatedly operated, managed, and assessed at the organizational level	CS-CMM Level 3 C2M2/C2M2-Nuclear MIL3 ENISA CSIRT Level 3 NIST CSF 2.0 Tier 3
Optimized	The optimized level at which security activities are continuously improved based on measurement and assessment results and feedback	CS-CMM Level 4 ENISA CSIRT Level 4 CMMC Level 3 NIST CSF 2.0 Tier 4

Baseline is the minimum operational level at which essential security activities for nuclear facility security are performed. Its core criteria include organizational structure, roles and responsibilities, identification of critical systems and critical digital assets, basic access control and security configuration, a basic detection environment, an incident reporting scheme, and minimum recovery measures. This level draws on the basic implementation stages of CS-CMM Level 2, C2M2/C2M2-Nuclear MIL1, ENISA CSIRT Level 1, and CMMC Level 1.

Developing is the level at which procedures, resources, and responsible structures for basic security activities are established, and activities are documented and initially operated. Its criteria include documented procedures, personnel training, drills and tools, riskbased prioritization, and initial operation by function. This level draws on the documentation and resourceestablishment stages of C2M2/C2M2-Nuclear MIL2 and ENISA CSIRT Level 2, and the riskinformed stage of NIST CSF 2.0 Tier 2.

Managed is the level at which security activities are repeatedly operated, managed, and assessed at the

organizational level. Its criteria include the periodic review of governance and risk management, periodic asset and risk analysis, repeated assessment of security baselines and access control, central monitoring, and the formalization of incident reporting procedures. This level draws on the standardized and organizationlevel management stages of CS-CMM Level 3, C2M2/C2M2-Nuclear MIL3, ENISA CSIRT Level 3, and NIST CSF 2.0 Tier 3.

Optimized is the level at which security activities are continuously improved based on measurement and assessment results and feedback. Its criteria include the periodic updating of risk and threat analysis information, the reporting and dissemination of assessment results and followup actions, the reflection of control effectiveness assessment results, and improvement based on external audits and feedback. This level draws on the measurement, feedback, and continuous improvement stages of CS-CMM Level 4, ENISA CSIRT Level 4, and NIST CSF 2.0 Tier 4, while CMMC Level 3 partially corresponds to this level.

4.3 Requirement Derivation for the Maturity Model

This section derives assessment requirements from six existing maturity models and from two nuclear facility regulatory documents. Following the security requirement classification of Firesmith [16], the derivation uses three criteria. The first is the protection target, which is the asset or information that a requirement protects. The second is the subject and scope of security application, which is the target and the extent to which a control applies. The third is the type of security activity, such as identification, access control, or monitoring. This process yields 40 requirements for CS-CMM, 30 for C2M2, 36 for C2M2-Nuclear, 41 for CMMC, 44 for ENISA CSIRT Capabilities, 27 for NIST CSF 2.0, 25 for TDL-005, and 26 for RG 5.71. The procedure for each model is described below.

In CS-CMM, requirements are arranged by level within each domain, and a higher level adds scope expansion or quantitative management on top of the lower levels. Requirements in the same domain and level that share a protection target are integrated into a representative requirement, whereas requirements at different levels are kept separate. This yields 40 requirements across ten domains and four levels.

In C2M2, every domain has a separate Management Activities Objective, and the Practices of this objective, which include procedure documentation, policy establishment, and effectiveness assessment, are placed at MIL2 or above. Objectives that differ in protection target or in activity type are kept separate, while Practices in the same Objective and MIL are integrated. This yields 30 requirements across ten domains from MIL1 to MIL3. Applying the same method with the added PHYSICAL and EXTENT domains yields 36 requirements across twelve domains for C2M2-Nuclear.

CMMC presents requirements across fourteen domains, and each requirement is fixed at one of its three levels. Within a domain and level, requirements that share a protection target, a subject, and an activity type are integrated, while requirements that differ in an essential way are kept separate. This yields 41 requirements.

In ENISA and SIM3, parameters fall into four categories, which are Organisation, Human, Tools, and Processes, and each parameter has an individual minimum certification level. Some parameters are kept separate because their protection target and purpose differ even though their activity type is similar. Integrating within each category and judging separation for adjacent parameters yields 44 requirements, comprising 10 in Organisation, 7 in Human, 10 in Tools, and 17 in Processes.

NIST CSF 2.0 presents subcategories, which are outcomes, across six functions, and each function is subdivided into categories. Integration is performed within each category, while physical and environmental controls that differ in an essential way in protection target or subject are kept separate from logical controls. This yields 27 requirements.

TDL-005 divides nuclear facility incident response into five stages and presents the tasks of each stage according to the responsibility of operators, regulatory bodies, and technical support organizations. Separating tasks that have different activity types, such as reporting, data collection, test environment setup, threat analysis, and mitigation, yields 25 requirements across the five stages.

RG 5.71 presents requirements across the nuclear facility cybersecurity program. These cover the cybersecurity organization, the identification of critical systems and critical digital assets, the defenseindepth strategy, security measures, incident and contingency planning, monitoring, personnel security, configuration management, supply chain management, and security assessment and risk management. Reconstructing the applicable requirements yields 26 requirements.

4.4 Mapping of Requirements to Maturity Levels by Function

The derived requirements are first assigned to a function. Referring to the six functions of Section 4.1 and to the subcategories of NIST CSF 2.0, each

Table III: Mapping of Maturity Model Requirements to Maturity Levels by Function

Function / Level	Baseline	Developing	Managed	Optimized
Govern	Establishes a dedicated cybersecurity organization, roles and responsibilities, policies, procedures, and incident and contingency plans as a minimal governance basis.	Extends risk management and supply chain risk management across the organization and documents the security policy.	Periodically reviews and assesses risk management activities and response plans. Documents the organization's delegation basis and collaboration scheme to operate governance systematically.	Adjusts response plans and controls to reflect threat and assessment changes, and continuously improves supply chain risk management and governance.
Identify	Identifies protection targets such as critical systems and critical digital assets. Provides a basic risk identification procedure and a minimal postreview scheme.	Adds threat exposure and prioritization to the asset inventory, and extends risk identification through accesspath and vulnerabilitysource analysis.	Periodically reviews and updates the asset inventory and risk analysis. Assesses the effectiveness of response activities and documents the results of followup actions.	Disseminates lessons learned from incidents, updates threat assessments, and advances risk identification through external audits and feedback.
Protect	Applies minimum protection measures, including access control, security training, patch management, basic configuration, and data backup.	Provides accessright review and threatexposurebased configuration, and extends personnel training and recruitment strategies.	Periodically updates, reviews, and tests security baselines, access control, and training content. Repeatedly manages whether protection measures function correctly.	Applies mandatory protection to all users and systems, and improves protection scheme through thirdparty extension and external verification.
Detect	Centralizes logs of critical systems and establishes a basic monitoring scheme. Secures a minimal detection foundation for identifying incidents and suspicious activities.	Establishes a threat profile to monitor and analyze information sources. Extends detection and analysis capability by, for example, analyzing the causes and paths of incidents.	Repeatedly operates central monitoring and log and anomalousbehavior analysis for the entire environment. Systematically performs assessment of security controls.	Applies automated detection techniques and continuous monitoring of asset changes. Advances detection capability through advanced risk assessment and security verification.
Respond	Provides an incident reporting scheme and performs minimal initial response, including containment that places the facility in a safe state when safety functions may be threatened.	Provides an integrated cyberphysical response scheme and mitigation measures. Extends initial response capability by preparing response tools and procedures.	Repeatedly manages incident handling with stakeholders after incident declaration, tracks mitigation effectiveness, and formalizes reporting and sharing.	Adjusts response strategies to reflect threat information. Continuously strengthens response capability through advanced detection techniques and recurrenceprevention measures.
Recover	Performs minimal recovery measures, such as reconstructing systems from trusted copies.	Performs recovery by introducing new assets when necessary. Extends recovery capability by establishing a business continuity plan.	Verifies recovered asset integrity, and manages recovery by documenting postincident operational and recoverytermination criteria based on cybersecurity risk.	Improves the plan by comparing recovery test results with objectives. Shares recovery progress by reflecting external verification results.

requirement is assigned to the function whose protection target and activity type match. The assigned requirements are then mapped to a level according to the criteria of Section 4.2, and each requirement is placed in Baseline, Developing, Managed, or Optimized.

Because the sources differ in purpose and structure, a requirement is assigned to a level by one of two methods. For CS-CMM, C2M2, C2M2-Nuclear, CMMC and SIM3, which define level schemes of their own, the native level is carried over: CS-CMM Level 2, MIL1, CMMC Level 1 and SIM3 level 1 correspond to Baseline; MIL2 and SIM3 level 2 to Developing; CS-CMM Level 3, MIL3, CMMC Level 2 and SIM3 level 3 to Managed; and CS-CMM Level 4, CMMC Level 3 and SIM3 level 4 to Optimized. For NIST CSF 2.0, TDL-005 and RG 5.71, which define no levels, each requirement is assigned to the level whose definition in Section 4.2 matches its content. Where the two methods disagree, the definitions of Section 4.2 take precedence; C2M2 THREAT MIL3, for example, requires vulnerability assessment by an independent party and review of the effectiveness of response, and is therefore placed at Optimized rather than at Managed. Requirements that describe the absence of an activity, such as CS-CMM Level 1 and MIL0, lie below Baseline and are not mapped.

Overlaps are resolved in two steps. A requirement whose protection target and activity type satisfy more than one function is assigned to each of those functions. For instance, the detection and removal of malicious code in RG 5.71 covers both a detection activity and an initial response activity, and is therefore placed in the Baseline of both Detect and Respond. A requirement is never assigned to more than one level within the same function, since the levels are cumulative. Requirements from different sources that then occupy the same function and level and share a protection target and activity type are merged into a single integrated requirement, and the identifiers of the contributing requirements are retained so that its origin remains traceable. When the merged requirements come from

different native levels, the integrated requirement takes the highest of them.

The Govern, Identify, and Protect functions concentrate requirements on organization, assets, risk management, access control, and training, which most models address in common. These sources include most domains of CS-CMM and C2M2 and C2M2-Nuclear, such as Asset, Risk, and Access, as well as CMMC, RG 5.71, and the Organisation and Human categories of ENISA. These functions span all four levels.

The Detect function is distributed across the four levels and centers on the THREAT and SITUATION domains of C2M2 and C2M2-Nuclear and on the AU, RA, CA, and SI domains of CMMC. The Respond and Recover functions are derived from the response and recovery requirements of NIST CSF 2.0, C2M2 and C2M2-Nuclear, and ENISA, together with the nuclear incident response requirements of TDL-005 and RG 5.71. In particular, the containment stage of TDL-005 reflects the nuclear specific characteristic of placing the facility in a safe state when safety functions are threatened. Table 3 shows the results.

The differing purposes of the sources are reflected in this distribution rather than in conflicts between them: the CMMC requirements fall almost entirely in Protect and Detect, the SIM3 parameters in Govern, Protect and Respond, and the TDL-005 tasks in Identify, Detect, Respond and Recover, while NIST CSF 2.0 is the only source distributed over all six functions. No single source covers the six functions, which is what the integration supplies.

5. Case Study

5.1 Application of the Proposed Maturity Model to RG 5.71

This section applies the proposed model to RG 5.71, a nuclear facility regulatory guide issued by the NRC, to illustrate the maturity levels expected for a nuclear facility that satisfies its cybersecurity requirements. RG 5.71 details methods for meeting 10 CFR 73.54 and is used for cybersecurity plans and regulatory review of nuclear power plants in the United States. The case study therefore maps the cybersecurity requirements represented by RG 5.71 to the proposed function and level scheme; it does not directly measure the operational maturity of a specific facility.

For each function and level, the assessment determines whether the cybersecurity requirements represented by RG 5.71 satisfy the integrated criteria of the proposed model. Because a lower level is a prerequisite for a higher level, the expected maturity level for an RG 5.71compliant facility is defined as the highest level that is continuously satisfied. A level is not assigned when its advanced integrated requirements are unmet. In Table 4, O indicates satisfied and X indicates not satisfied.

Table IV: Application of the Proposed Model to RG 5.71

Function / Level	Baseline	Developing	Managed	Optimized	Achieved Level
Govern	O	O	O	O	**Optimized**
Identify	O	O	O	X	**Managed**
Protect	O	O	O	X	**Managed**
Detect	O	O	O	X	**Managed**
Respond	O	O	O	X	**Managed**
Recover	O	O	O	X	**Managed**

Under the proposed model, a facility satisfying RG 5.71 would correspond to the Optimized level for the Govern function and the Managed level for the other five functions. For Govern, RG 5.71 establishes governance through security assessment and authorization, policies and procedures, and roles and responsibilities. It periodically reviews risk management and response plans, and through periodic program review and a corrective action program it continuously adjusts and improves controls and response plans to reflect changes in threats and assessment results. These requirements correspond to the Optimized level of Govern.

For Identify, Protect, Detect, Respond, and Recover, RG 5.71 requires the identification and validation of critical digital assets with periodic review of risk analysis, the application and periodic testing of access control, training, and baselines, continuous monitoring and effectiveness analysis, the establishment and testing of incident response with corrective action, and a recovery plan that ensures the continuity of SSEP functions and is managed through corrective action. For an RG 5.71compliant facility, these activities correspond to the Managed level, at which security activities are repeatedly operated and managed at the organizational level. However, RG 5.71 does not explicitly require the advanced elements added at the Optimized level. Identify does not require continuous advancement through external audits and feedback; Protect does not require extension to third parties and external verification; Detect does not require advanced automated detection and correlation; Respond does not require continuous adjustment of response strategy from threat information; and Recover does not require improvement based on comparison with objectives and external verification. These five functions therefore remain at the Managed level.

For example, the continuous monitoring and assessment requirements of RG 5.71 automatically collect and analyze network traffic and the events and logs of critical digital assets to notify security events in real time, and they periodically analyze the effectiveness of security controls. When these requirements are mapped to the proposed model, an RG 5.71compliant facility corresponds to the Managed level of Detect, which repeatedly operates central

monitoring, log and anomaly analysis, and systematic assessment of security controls. The Optimized level of Detect additionally requires advanced automated techniques such as machinelearningbased anomaly detection or automatic correlation. Because RG 5.71 does not explicitly require these advanced techniques, Detect remains at the Managed level.

In summary, under the proposed model, a facility satisfying RG 5.71 would correspond to Optimized for Govern and Managed for the other five functions. Govern reaches Optimized through periodic review and continuous improvement, while the others remain Managed because RG 5.71 does not explicitly require advanced automation, external verification, and feedback across those functions. The case study thus illustrates function-level maturity expected from RG 5.71 compliance rather than directly measuring the operational maturity of a specific nuclear facility.

5.2 Example of Integrated Interpretation

Through a hypothetical scenario, this section shows how the model integrates and interprets, in one consistent form, the results of frameworks that have different structures and level schemes. We suppose that a facility A independently performed a C2M2 selfassessment and an RG 5.71 based regulatory check.

In the C2M2 selfassessment, the THREAT and SITUATION domains remain at MIL1 because the Practices at MIL2 and above are not sufficiently implemented. This means that basic activities exist but that threat information, situation awareness, and monitoring are not yet documented or systematized.

RG 5.71 requires the monitoring of critical digital assets and action on external security information. In the regulatory check, facility A does not satisfy these requirements. This means that its capability to continuously identify anomalies and to reflect external threat information is insufficient.

Because one result is expressed as a C2M2 MIL rating and the other as RG 5.71 satisfaction, the two are difficult to compare directly, but both map to the Detect function. The MIL1 rating of the Threat and Situation domains corresponds to the Baseline of Detect but does not reach the threat analysis and continuous monitoring of Developing. The monitoring and external information requirements that are unmet in RG 5.71 are also core to Detect. The Detect function of facility A therefore stays at the Baseline level, and advancing to Developing requires strengthening threat analysis, continuous monitoring, and security information based action.

The model thus interprets results more holistically than using models separately. Rather than reading a C2M2 MIL rating and RG 5.71 satisfaction apart, it converts both into the same functions and levels under one criterion. Because levels are determined by function, it also reduces the problem of a weak function being masked in the overall result. In this case, the Detect function of facility A is revealed as Baseline, which exposes a weakness in detection even when other functions are strong.

6. Conclusion and Future Works

We derived requirements from CS-CMM, C2M2, C2M2-Nuclear, CMMC, ENISA CSIRT Capabilities, and NIST CSF 2.0, and from the nuclear regulatory documents IAEA TDL-005 and NRC RG 5.71. On this basis, we developed a nuclear cybersecurity maturity model that integrates the requirements into six functions and four levels: Baseline, Developing, Managed, and Optimized. Applying the model to RG 5.71 showed that a compliant nuclear facility would correspond to Optimized for Govern and Managed for the other five functions. The hypothetical scenario further showed that results expressed using different domains and maturity schemes can be mapped and interpreted under a common structure.

The main contributions of this paper are as follows. First, we presented the characteristics of nuclear facilities that distinguish them from general IT and ICS environments, and we showed that the model reflects them. Second, we jointly derived and integrated, from regulatory documents, the safety linkage and compliance requirements that general models cannot capture on their own. Third, by converting results from different domains and level schemes into six functions, we established a basis for consistent comparison across frameworks.

Because the assessment is performed at the requirement level, detailed controls may collapse into single function-level cells, and integrating different level schemes may simplify some distinctions. Future work will extend the mapping to detailed subitems and validate the model through multiple case studies and independent evaluations to improve the reproducibility and reliability of the mapping process.

ACKNOWLEDGMENT

This work was partly supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.RS-2026-25585348, Graduate School of Security Convergence(AI)(Gachon University), 50%) and Korea Foundation of Nuclear Safety(KoFONS) grant funded by the Korea government(NSSC) (No.RS-2026-25536917, Establishment of a cyber attack path and threat assessment database, 50%)

REFERENCES

[1] Stouffer, K., Pease, M., Tang, C.Y., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., Thompson, M.: Guide to Operational Technology (OT) Security. NIST Special Publication 800-82 Revision 3.

National Institute of Standards and Technology, Gaithersburg (2023)
[2] Christopher, J.D.: State of ICS/OT Security 2025. SANS (2025)
[3] International Atomic Energy Agency (IAEA): IAEA Nuclear Security Series No. 33T(Computer Security of Instrumentation and Control Systems at Nuclear Facilities). IAEA, Vienna (2018)
[4] Buzdugan, A., Căpățână, G.: The Trends in Cybersecurity Maturity Models. In: Education, Research and Business Technologies: Proceedings of the 21st International Conference on Informatics in Economy (IE 2022), pp. 217–228. Springer (2023)
[5] International Atomic Energy Agency (IAEA): IAEA Nuclear Security Series No. 17T(Computer Security Techniques for Nuclear Facilities). IAEA, Vienna (2021)
[6] Liyanage, L., Arachchilage, N.A.G., Russello, G.: SoK: Identifying Limitations and Bridging Gaps of Cybersecurity Capability Maturity Models (CCMMs). arXiv:2408.16140 (2024)
[7] New Zealand National Cyber Security Centre: Cyber Security Capability Maturity Model (CS-CMM) and Minimum Cyber Security Standards. New Zealand National Cyber Security Centre, Wellington (2025)
[8] U.S. Department of Energy: Cybersecurity Capability Maturity Model (C2M2), Version 2.1. U.S. Department of Energy, Washington, DC (2022)
[9] Pacific Northwest National Laboratory: Cybersecurity Capability Maturity Model for the Nuclear Sector (C2M2-Nuclear), Version 1.0 User Guide. Pacific Northwest National Laboratory, Richland (2023)
[10] U.S. Department of Defense: Cybersecurity Maturity Model Certification (CMMC) Program. Federal Register 89(199), 83092–83220 (2024)
[11] European Union Agency for Cybersecurity (ENISA): CSIRT Capabilities: How to Assess Maturity? Guidelines for national and governmental CSIRTs. ENISA, Heraklion (2015)
[12] Stikvoort, D.: SIM3 : Security Incident Management Maturity Model. Open CSIRT Foundation (2015)
[13] National Institute of Standards and Technology: The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Paper 29. National Institute of Standards and Technology, Gaithersburg (2024)
[14] International Atomic Energy Agency: Computer Security Incident Response Planning at Nuclear Facilities. IAEATDL-005. International Atomic Energy Agency, Vienna (2016)
[15] U.S. Nuclear Regulatory Commission: Cybersecurity Programs for Nuclear Reactors. Regulatory Guide 5.71. U.S. Nuclear Regulatory Commission, Washington, DC (2023)
[16] Firesmith, D.G.: A Taxonomy of SecurityRelated Requirements. In: Proceedings of the International Workshop on High Assurance Systems (RHAS'05), pp. 29–30 (2005)