Analysis of Security Guidelines for Exploring Improvements in Nuclear Facility Network Defense Architecture

Dongmin Kim[a], Moohong Min[b*], and Aram Kim[c*]
[a]*Sungkyunkwan Univ., Immersive Media Engineering Dept., 25-2 Sungkyunkwan-ro, Seoul, 03063*
[b]*Sungkyunkwan Univ., Computer education Dept./Social innovation Convergence Program, 25-2 Sungkyunkwan-ro, Seoul, 03063*
[c]*University of Suwon, Information Security Dept., 17 Wauan-gil, Hwaseong-si, 18323*
[*]*Corresponding authors: iceo@skku.edu and aramkim@suwon.ac.kr*

Keywords : Network Defense Architecture, Defense-in-Depth, Boundary Protection, International Guidelines

1. Introduction

Cyberattacks targeting nuclear facilities have increasingly raised concerns about the security of nuclear power plants (NPPs). Notable incidents, such as the Stuxnet attack on Iran's nuclear enrichment facilities and the cyber intrusion against Korea hydro & nuclear power and its contractors, highlight critical vulnerabilities in nuclear infrastructure [1]. These threats pose significant risks to the integrity of safety-critical systems in NPPs, underscoring the necessity for robust cybersecurity measures in digital control environments.

This study focuses on enhancing defense-in-depth protection architecture as key area for investigation and improvement. By analyzing established guidelines on defense-in-depth cybersecurity frameworks, this research aims to propose advancements in network defense architectures specifically tailored for nuclear facilities. Furthermore, our analysis extends to Korea's nuclear security standards, identifying potential enhancements by integrating key elements from security guidelines. The findings contribute to strengthening the cybersecurity resilience of NPPs in Korea, ensuring their safe and secure operation in an evolving threat landscape.

2. Background

This section outlines the concepts of defense-in-depth protective architecture and boundary protection technologies, which are mainly discussed in this paper.

2.1 Defense-in-Depth

The U.S. nuclear regulatory commission (NRC) regulatory guide (RG) 5.71 [2] mandates the implementation of a defense-in-depth protective strategy to safeguard critical digital assets (CDAs) in NPPs. CDAs encompass digital assets associated with safety, security, and emergency preparedness functions.

This strategy involves the application of multiple layers of defense mechanisms designed to detect, prevent, respond to, mitigate, and recover from cyberattacks. The implementation approach includes establishing multiple formal communication boundaries to construct a defensive architecture comprising distinct security levels. Networks can be segmented into different zones which logically correspond to the physical security zones within the facility. Boundary control devices enforce one-way communication from Level 4 to Level 3 and Level 3 to Level 2, for protecting higher levels which include CDAs, which generally operate according to “deny-all, permit-by-exception” policy. These devices regulate unidirectional communication, such as Level 4 to Level 3. An example of the defense-in-depth protective architecture incorporating these concepts is illustrated below:

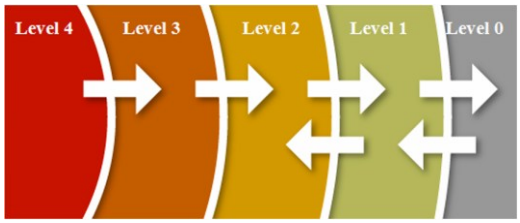

Fig. 1. Example of defense-in-depth protective architecture [2]

2.2 Boundary Protection Technologies

Boundary protection technologies encompass the tools used to secure network boundaries during implementation of defense-in-depth architecture. These technologies play a critical role in controlling and monitoring network communications across these boundaries. One prominent example of boundary protection technologies is one-way communication devices.

The concept of one-way communication applied in nuclear facilities is outlined in IEEE 7-4.3.2 (Standard for digital computers in safety systems of nuclear Power generating stations) [3]. The standard mandates communication isolation between safety systems and non-safety systems to mitigate the risk of propagating cyberattacks. It assumes that safety functions performed by safety systems should not rely on inputs from non-safety systems, and that data should be transmitted in a unidirectional manner.

RG 5.71 also endorses this approach and recommends the use of hardware that enforces one-way communication. A key example of such hardware is a data diode, which is designed to enforce unidirectional data flow at the physical level by physically removing

the receiver component from the hardware, thereby preventing bidirectional communication.

3. Analysis of Guidelines

3.1 IAEA Nuclear Security Series No. 17-T (Rev. 1)

The Nuclear Security Series consists of publications issued by the International Atomic Energy Agency (IAEA) to prevent and detect unauthorized activities involving nuclear materials and facilities. Among these, Guidance No. 17-T (Rev. 1) (hereafter referred to as NSS 17-T) [4] provides key recommendations for enhancing defense-in-depth architecture.

NSS 17-T employs a graded approach to system protection by defining computer security levels and computer security zones. Security levels are determined based on the protection requirements for specific physical and logical areas, with Level 1 imposing the most stringent security measures. Additionally, computer security zones and detailed systems are classified according to these levels.

The guidance emphasizes the nuclear facility zone model, which, while sharing commonalities with other guidelines–such as restricting communication to a unidirectional flow between computer security zones of different levels–introduces a more refined segmentation strategy. Notably, this model mitigates error propagation by ensuring separating zones and systems even within the same security level. For zones in Level 1 and 2, the guidance recommends minimizing interactions with other zones, including those at the same level. Conversely, for higher-risk zones (Level 4 and 5), which are more vulnerable to cyberattacks, it advocates implementing proactive detection capabilities to identify and mitigate cyber threats.

By adopting this approach, the defense-in-depth architecture can be more granularity, ensuring that security requirements are precisely aligned with the specific characteristics and risk profiles of each level and zone.

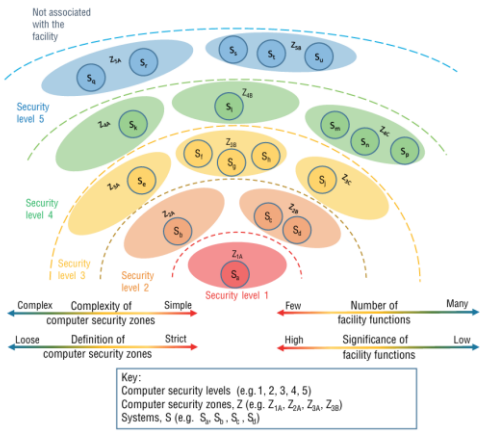

Fig. 2. Conceptual model of computer security levels and zones in NSS 17-T [4]

3.2 IEC 62443-1-1

IEC 62443-1-1 [5] is a guidance document developed by the International Electrotechnical Commission (IEC), that addresses key concepts and models related to the security of Industrial Automation and Control Systems (IACS). Similar to other security frameworks, it segments networks into security zones but introduces the distinct concept of a conduit, a specialized type of security zone designed to control communication within or between zones.

A conduit is defined as a grouping of information flows and consists of multiple individual flows, referred to as channels. As shown in Fig.3, conduits can either cross zone boundaries (e.g., Enterprise conduit) or exist within a single zone (e.g., Plant control conduit).

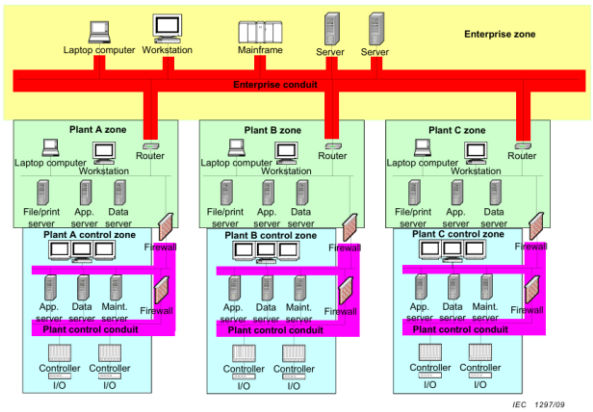

Fig. 3. Conduit example model in IEC 62443 1-1 [5]

Conduits are further classified as either trusted or untrusted. Plant control conduits are generally categorized as trusted conduits because they operate within a single security zone. However, the classification of Enterprise conduits depends on the underlying network infrastructure. If an Enterprise conduit is based on a wide area network, it can be considered as a trusted conduit. Conversely, if it involves a public network, it is classified as an untrusted conduit, necessitating the application of secure countermeasures at the channel level rather than treating the conduit as a single unit.

Table I: Trusted and untrusted conduit in Fig. 3.

Conduit	Trust level	Communication type
Enterprise conduit	Trusted	Data center to plant (private network based)
Enterprise conduit	Untrusted	Data center to plant (public network based)
Plant control conduit	Trusted	Within plant control zone

In IEC 62443-1-1, conduits are explicitly defined as pathways for data flow, emphasizing the necessity of applying individual security countermeasures to conduits, particularly where boundary protection technologies are deployed.

3.3 KINAC/RS-015

The Regulatory Standard on Computer Security of Nuclear Facilities (KINAC/RS-015) provides guidance on the defense-in-depth architecture in Korea, aiming to protect CDAs from cyberattacks as defined in the Design Basis Threat (DBT) [6]. This standard establishes cybersecurity levels ranging from Level 0 to Level 4, assigning CDAs responsible for safety-related and security functions to Level 4 and mandating that communication up to Level 2 must be strictly unidirectional. Notably, this approach aligns with the definition in RG 5.71, which similarly requires data transmission through a boundary protection system during communication.

To enhance the defense-in-depth architecture outlined in this standard, various studies have explored potential improvements. A notable approach involves introducing an additional security level and elevating vital digital assets (VDAs) to a higher level. VDAs refer to CDAs that are directly associated with incident response, and the proposed model separates VDAs from existing Level 4 CDAs, relocating them to a newly defined Level 5. This method creates an additional security zone, which differs in implementation from the other guidelines examined but could complement their architectural strategies.

3.4 Integrating measures for improving defensive architecture

Our analysis revealed complementary strengths across multiple standards and guidelines for enhancing nuclear facility protection. NSS 17-T introduces fine-grained zone segmentation, even within the same security levels, thereby providing enhanced protection against error propagation. This approach would enable RS-015 to implement more nuanced security measures within each level, rather than applying uniform protections to all assets at a given level.

IEC 62443-1-1 offers a structured classification framework for securing communication pathways, distinguishing between trusted and untrusted conduits that require different handling at the conduit unit or individual channel level. Integrating this concept into RS-015 would strengthen boundary protection by ensuring that appropriate security controls are applied to different communication pathways.

These architectural enhancements could reinforce RS-015's existing tiered approach, particularly when combined with the proposed elevation of VDAs to a higher security level. The resulting framework would establish a more robust and adaptable protection architecture for nuclear facilities.

4. Application case & Discussion

In this section, we examine an application case of network security architecture based on IEC 62443-1-1. B&R Industrial Automation GmbH (B&R), a company providing IACS solutions across various industries, advocates for a defense-in-depth strategy comprising six layers to ensure the security of its products [7].

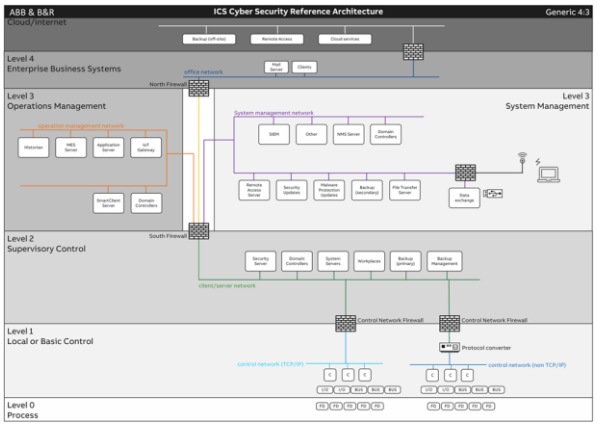

Fig. 4. Cyber Security Reference Architecture in B&R [7]

Depending on the application of the TCP/IP protocol between Level 1 and Level 2, traffic passes through different control network firewalls. Additionally, Level 3 is segmented within the same level in accordance with the scope of management, demonstrating that segmentation is tailored to B&R's IACS environments.

Analyzing architecture cases specifically applied to NPPs would be most effective. However, due to industry-specific constraints, acquiring practical examples is limited. Therefore, it is necessary to derive potential improvements applicable to NPPs based on cases of defense-in-depth implementation in other IACS environments such as B&R.

5. Conclusion

Given the growing need to enhance the protection architecture of nuclear facility networks, this study examined improvement measures for defense-in-depth architecture. By analyzing international guidelines, we defined the core concepts and applicable features that can enhance the RS-015 framework. In addition, we investigated real-world example in other industrial field, identifying practical features used in IACS environments. Integrating these features allowed us to propose a more robust and resilient protection architecture for nuclear facilities.

For future research, we will conduct an in-depth analysis of additional international guidelines and additional real-world implementations of protection architectures within diverse security frameworks.

Furthermore, we will investigate the characteristics of commercial off-the-shelf (COTS) products suitable for boundary protection and explore their potential integration with the mitigation strategies proposed in this study.

Acknowledge

This work was supported by the Nuclear Safety Research Program through the Korea Foundation Of Nuclear Safety (KoFONS) using the financial resource granted by the Nuclear Safety and Security Commission (NSSC) of the Republic of Korea. (No. RS-2024-00403596)

REFERENCES

[1] H. K. Lee, Suspected North Korean Hacking Attack…Leakage of 720,000 Nuclear Plant Documents, Korea Economic Daily, 09-Oct.-2024. [Online]. Available: https://www.hankyung.com/article/2024100945185.
[2] U.S. Nuclear Regulatory Commission, Nuclear Regulatory Commission Regulatory Guide 5.71 Revision 1, 2023.
[3] IEEE Power and Energy Society, IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations, 2016.
[4] International Atomic Energy Agency, Nuclear Security Series No. 17-T (Rev. 1): Computer Security Techniques for Nuclear Facilities, 2021.
[5] International Electrotechnical Commission, Industrial Communication Networks – Network and System Security – Part 1-1: Terminology, Concepts and Models, 2009.
[6] S. M. Kim, Regulation and Implementation of Cybersecurity Defense-in-Depth Strategy for Nuclear Power Plants, Transactions of the Korean Nuclear Society Spring Meeting, p. 771, 2021.
[7] B&R Industrial Automation GmbH, Cyber Security – Defense in Depth for B&R Products, 2024.