Analysis of the 2025 Poland Energy Sector Cyber Incident via Three Attack Models and Review of KINAC/RS-015 Regulatory Coverage

Minjung Kim [a*], Chaechang Lee [a]
[a]*Korea Institute of Nuclear Nonproliferation and Control (KINAC), Daejeon, Republic of Korea*
[*]*Corresponding author: kimmj421@kinac.re.kr*

***Keywords :** Cybersecurity, Poland Energy Sector, Attack Models, Nuclear Facilities, KINAC/RS-015

1. Introduction

Destructive cyberattacks increasingly target the Operational Technology (OT) and Industrial Control Systems (ICS) of critical infrastructure rather than solely its Information Technology (IT). While earlier attacks predominantly pursued financial extortion, recent intrusions have deliberately corrupted edge devices and halted critical physical processes, an escalation that observers now describe as "cyber arson."

The 29 December 2025 incident in Poland's energy sector revealed how far this escalation reached [1]. The intrusion exhibited tradecraft associated with known Advanced Persistent Threat (APT) clusters such as "Static Tundra" and "Sandworm." Crossing IT boundaries directly into OT environments, the attacker destroyed field devices, severed telecommunications, and erased remote monitoring and control capability.

This study evaluates how the Korean nuclear cybersecurity regulatory standard, KINAC/RS-015, addresses emerging physical-destruction attacks against OT environments. Structuring the observed incident techniques through three complementary attack models, the analysis maps each empirical attack vector directly onto a KINAC/RS-015 baseline control. This mapping then determines whether current regulatory requirements would have prevented operational disruption across the affected field devices.

2. Methods

Ten devices targeted in Poland's energy infrastructure incident served as the analytical cases. The initial report identified eight devices across five renewable Grid Connection Points (GCPs), two large Combined Heat and Power (CHP) plants, and one manufacturing facility [1]. The follow-up report added two devices from a smaller CHP plant [2].

The analysis integrated three widely used attack models: the Lockheed Martin Cyber Kill Chain, the MITRE ATT&CK Framework, and the Diamond Model [3]. Each model examines a cyberattack from a different vantage point through intrusion sequence, adversary technique, and environmental context, thereby providing a complementary view.

For each of the ten target devices, the analysis synthesized the three models to evaluate intrusion progression (Cyber Kill Chain), behavioral techniques (MITRE ATT&CK Framework), and environmental context (Diamond Model), isolating the primary vulnerability factor: the single precondition whose removal would collapse the attack.

The analysis then mapped the identified root causes onto KINAC/RS-015, the Korean nuclear cybersecurity regulatory standard adapted from the United States Nuclear Regulatory Commission (NRC) guidance. KINAC/RS-015 is fundamentally designed to prevent cyber sabotage that could compromise safety, security, and emergency preparedness functions or lead to radiological release.

2.1 Lockheed Martin Cyber Kill Chain

The Cyber Kill Chain structures a cyber intrusion as seven sequential phases, from reconnaissance to actions on objectives [4]. The model tracks how an attack advances along a chronological timeline and identifies where a defender can disrupt each stage. Its linear, sequence-driven design, however, does not resolve the granular protocol-level manipulations on field control devices into distinct phases. For each affected device, the analysis applied the Kill Chain to determine how far the intrusion advanced through the seven phases.

2.2 MITRE ATT&CK Framework

MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) is a globally accessible knowledge base that organizes real-world adversary behavior into standardized tactics and techniques, commonly referenced as Tactics, Techniques, and Procedures (TTPs) [5]. The Enterprise matrix covers IT environments and host-level actions, while the ICS matrix extends this coverage to actions against field control devices and physical processes. ATT&CK labels each observed behavior with a standardized technique identifier, the granularity that mapping behavior to specific security controls requires. The framework, however, does not represent the end-to-end timeline or the relational causality linking these techniques. For each device, the analysis applied ATT&CK to describe the observed behavior as standardized techniques.

2.3 Diamond Model

The Diamond Model structures a cyber event around four core features: adversary, capability, infrastructure, and victim [6]. The model captures the relationships among these features, showing how an adversary applies a capability against a victim rather than following a linear event sequence. On its own, however, the model provides neither a chronological timeline nor granular technical classification. Because this study treated the adversary as a single actor across all devices, the analysis applied the Diamond Model to examine how the capability engaged each victim device and its operating environment.

3. Results and Discussion

The analysis of the ten target devices revealed an initial entry vulnerability across all cases: the adversary gained initial access through Internet-facing perimeter Virtual Private Network (VPN) firewalls that lacked Multi-Factor Authentication (MFA). Thereafter, however, the attack paths differed markedly depending on device category (Remote Terminal Unit (RTU), Programmable Logic Controller (PLC), Intelligent Electronic Device (IED), serial server) and operating environment. The analysis presents the multi-model attack progressions for two representative OT field devices that suffered physical impact (Table I).

Table I: Analysis of targeting cases (partial)

Device	Hitachi RTU560	Siemens S7-300/1200/1500
Facility	Renewable GCPs	CHP Plant
Cyber Kill Chain	Step 7. Actions on Objectives (Device Brick)	Step 7. Actions on Objectives (Turbine/Water Shutdown)
MITRE ATT&CK	T0812 Default Credentials	T0846 Remote System Discovery
	T0857 System Firmware Corruption	T0886 Remote Services
	T0827 Loss of Control	T0855 Unauthorized Command Message
	T0829 Loss of View	T0858 Change Operating Mode
	T0816 Device Restart/Shutdown	T0813 Denial of Control
	-	T0826 Loss of Availability
	-	T0828 Loss of Productivity
Diamond Model	Capability: Corrupted firmware (0xFF, 240 B) + default credentials	Capability: Native Siemens S7 communication protocol commands (Living-off-the-Land)
	Victim: RTU web/maintenance interface	Victim: Steam turbine and water treatment logic
	Mechanism: Unvalidated firmware image upload → endless reboot loop	Mechanism: Misconfigured cellular APN route → direct unauthorized STOP commands and password locking

By synthesizing all three analytical lenses for each device, the primary vulnerability factor emerges directly.

Hitachi RTU560 (Firmware Corruption): The Cyber Kill Chain placed the attack at Step 7 (Actions on Objectives). MITRE ATT&CK decomposed the physical disruption (T0827, T0829, T0816) into the malicious firmware modification technique (T0857) executed through default credentials (T0812). The Diamond Model linked this capability to the web update interface, identifying the payload as a malformed 240-byte binary filled with 0xFF. Synthesizing these three findings demonstrates that the entire destructive chain hinged on the device accepting the corrupted binary without cryptographic verification. Even after the adversary penetrated the perimeter and supplied default credentials, enforcing cryptographic signature and hash verification at the firmware update interface would have rejected the bogus payload, collapsing the Actions on Objectives phase. The primary vulnerability factor therefore reduces to the absence of firmware-integrity verification.

Siemens S7 Controllers (Native Protocol Abuse): The Cyber Kill Chain placed the attack at Step 7 (Actions on Objectives), which halted physical processes. MITRE ATT&CK showed that the physical impact (T0813, T0826, T0828) stemmed from unauthorized operational mode changes (T0858 STOP) transmitted via remote services (T0886). The Diamond Model clarified the operational context: the adversary executed standard, unauthenticated S7 protocol commands (living off the land) through a Secure Shell (SSH) tunnel traversing an unisolated private cellular Access Point Name (APN). Cross-analyzing these three dimensions reveals that because the controllers inherently execute valid native commands, endpoint filtering offered no defense. The entire attack sequence depended strictly on network reachability across an unsegmented boundary. Enforcing boundary isolation would have severed the communication path before any native command reached the PLC. The primary vulnerability factor therefore reduces to direct network access via an unisolated cellular connection.

Table II: RS-015 coverage for targeting cases

Device	Hitachi RTU560	Siemens S7-300/1200/1500
Primary Vulnerability Factor	Firmware-integrity verification absent (secure update disabled)	Direct network access via an unisolated cellular connection
KINAC/ RS-015	Sec. 2.2.6.2.6 System Hardening	Sec. 2.2.6.2.2 Access Control
	App.2. 1.5.3 File System & OS Change Authorization App.2. 1.5.5 OS, Application, and Third-Party Software Installation and Updates	App.2. 1.1.12 Network Access Control App.2. 1.1.14 Prohibition of Wireless Connections

Table II summarizes the regulatory coverage of KINAC/RS-015 mapped against the identified primary vulnerability factors. Enforcing baseline requirements—specifically System Hardening (Sec. 2.2.6.2.6), File System and Operating System Change Authorization (App. 2, Sec. 1.5.3), OS, Application, and Third-Party Software Installation and Updates (App. 2, Sec. 1.5.5), Access Control (Sec. 2.2.6.2.2), Network Access Control (App. 2, Sec. 1.1.12), and Prohibition of Wireless Connections (App. 2, Sec. 1.1.14)—would have preempted these representative attack vectors prior to physical disruption. Furthermore, KINAC/RS-015 baseline controls comprehensively govern the remaining eight affected devices, neutralizing the corresponding exploitation techniques. Consequently, rigorous enforcement of KINAC/RS-015 requirements would have prevented physical operational disruption across all ten evaluated devices. The Polish incident underscores that even elementary administrative oversights can catalyze severe operational collapses, reinforcing that robust defense demands strict boundary isolation across every external OT interface.

4. Conclusions

The analysis evaluated ten compromised devices from Poland's energy sector incident through the complementary frameworks of the Lockheed Martin Cyber Kill Chain, MITRE ATT&CK, and the Diamond Model. Mapping the empirical attack vectors directly to KINAC/RS-015 demonstrates that existing regulatory baseline controls would sufficiently mitigate emerging OT-targeted physical destruction attacks across both IT and field environments, provided they are rigorously enforced. These findings provide an empirical foundation for future regulatory enhancements, including regulatory inspections, Design Basis Threat (DBT) updates, and specialized inspector training programs.

Acknowledgements

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. (RS-2026-25535614)

REFERENCES

[1] CERT Polska, Energy Sector Incident Report - 29 December 2025, Technical Report, pp. 1-46, 2026.
[2] CERT Polska, Follow-Up Analysis of the 29 December 2025 Energy Sector Incident, Technical Report, pp.1-19, 2026.
[3] N. Naik et al., Comparing Attack Models for IT Systems: Lockheed Martin's Cyber Kill Chain, MITRE ATT&CK Framework and Diamond Model, IEEE International Symposium on Systems Engineering (ISSE), pp. 1-6, 2022.
[4] E. M. Hutchins et al., Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, Leading Issues in Information Warfare & Security Research, Vol. 1, pp. 80-106, 2011.
[5] O. Alexander et al., MITRE ATT&CK for industrial control systems: Design and philosophy, Report No. MP0155863, The MITRE Corp., pp. 1-43, 2020.
[6] S. Caltagirone et al., The Diamond Model of Intrusion Analysis, Technical Report, pp. 1-61, 2013.