Maintaining Nuclear Security during Decommissioning : A Comprehensive Analysis of WINS Guide 4.13

Young-Il Na[a*], Hyung-Woo Seo [a], Chan-Geun Park[a], and Gang-Woo Ryu[a]
[a]*Korea Hydro & Nuclear Power (KHNP) Central Research Institute, 70, 1312-gil, Yuseong-daero, Yuseong-gu, Daejeon, 34101, Republic of Korea*

Keywords : IAEA, WINS Guide

1. Introduction

Decommissioning is the final step in the nuclear facility lifecycle. Traditionally, emphasis has been placed on safety and radiological protection. However, the assumption that security risks diminish after permanent shutdown is misleading. While nuclear fuel inventories decrease, decommissioning introduces new risks: an expanded contractor workforce, large-scale material movements, increased reliance on digital planning systems, and potential complacency within downsized organizations.

International bodies such as the IAEA highlight the importance of nuclear security during all lifecycle stages (NSS 35-G). WINS Guide 4.13 builds upon these principles by offering a practical roadmap for sustaining effective security measures during decommissioning.

2. Methods and Results

1. Scope of WINS Guide 4.13

The WINS Guide 4.13 applies to a broad range of facilities: commercial nuclear power plants, research reactors, and fuel cycle installations. It addresses three dimensions of security:

① Physical Security – barriers, detection systems, armed response, and access control.
② Cybersecurity – protection of monitoring, planning, and data management systems.
③ Information Security – safeguarding sensitive design drawings, decommissioning schedules, and transport data.

The guide also introduces two tools:

- A self-assessment survey, enabling organizations to benchmark practices.
- A five-level maturity scale, helping operators track progress and identify areas for improvement.

① Phiysical Security

Physical security refers to the defense measures designed to protect critical assets such as residual nuclear fuel, radioactive materials, essential equipment, and sensitive information.

- The importance of physical security evolves throughout decommissioning:
- Early Stage (Post-Shutdown): High-risk phase due to presence of nuclear fuel and significant radioactive materials. Maximum security must be maintained.
- Fuel Removal Phase: Transport security becomes critical, including confidential routing, armed escorts, and contingency planning.
- Decommissioning and Decontamination: Focus shifts to managing a surge of contractors and workers. Insider threat prevention and access control are crucial.
- Final Stage (Pre-Site Release): Fewer nuclear assets remain, but monitoring of residual waste and sensitive documentation is required. Security can be gradually scaled down, but oversight must continue.

Physical security during decommissioning must integrate detection, delay, and response in a dynamic, risk-based framework. Even as radioactive material inventories decrease, the risk shifts toward insider threats, material diversion, and information leaks—making physical protection an enduring priority.

② Cybersecurity

If Physical Security is the visible wall and guard system, then Cybersecurity is the invisible shield that protects all the digital veins running through a decommissioning project. WINS Guide 4.13 emphasizes that cyber risks grow as facilities rely more heavily

on digital systems for planning, monitoring, and material control.

For Example, our plant have Digital Control System, Inventory Database, Logistics & Planning Tools and Communications & Security Networks.

Cybersecurity in decommissioning is about protecting the digital nervous system of a dismantling project. Without it, physical security can be undermined, sensitive data can be weaponized, and adversaries can exploit vulnerabilities in ways invisible to guards and cameras. WINS Guide 4.13 urges operators to treat cyber protection not as an add-on, but as a core component of nuclear security.

③ **Information Security**

Nuclear decommissioning generates and uses a massive amount of sensitive information. Therefore, information security is not limited to digital data but also includes physical documents, drawings, and verbal communications.

Information security during decommissioning safeguards the knowledge itself that could enable an attack or diversion. WINS Guide 4.13 stresses that without strong controls on documents, data, and communications, both physical and cyber measures can be undermined. Protecting information is therefore a cornerstone of nuclear security resilience.

3. Conclusions

Decommissioning is a phase of changing threats, not diminished threats. WINS Guide 4.13 highlights that nuclear security must remain central until the final release of a site. Its checklist-based methodology and maturity framework provide operators with both tactical guidance and strategic direction. By embedding a graded, integrated, and culture-focused approach, facilities can ensure nuclear security resilience throughout the decommissioning journey.

REFERENCES

[1] WINS Guide 4.13, Maintaining Effective Security during the Decommissioning of Nuclear Power Plants, World Institute for Nuclear Security, 2020.
[2] IAEA, Nuclear Security Series No. 35-G: Security of Nuclear Facilities during Lifetime Stages, 2018.
[3] IAEA, INFCIRC/225/Rev.5: Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities, 2011.