Security Considerations for the "Nuclear Reactors, Materials, and Waste" Sector

Delgerekh Ariunbileg

November 19, 2025

1 Introduction

This paper presents a cybersecurity risk assessment for the **Nuclear Reactors, Materials and Waste** Critical Infrastructure Sector, an essential sector of national security that supports economic stability and public safety. This sector, which is overseen by the Nuclear Regulatory Commission (NRC) and supported by the Department of Energy (DOE), produces vital energy and materials while managing significant public safety concerns.

The analysis identifies the **physical infrastructure of nuclear reactors** as a highly critical asset and integral to energy production while categorizing **intellectual property/classified information** as a medium-criticality asset enabling innovation. Security regulations, such as those set in 10 CFR § 73.27(b) and § 73.54(d)(2), require strict protocols for material oversight and mandatory cybersecurity training for employees.

Key threats include the rigid and sensitive nature of **Distributed Control Systems (DCS)** within facilities and the persistent risk of **insider threats**. These threats exploit vulnerabilities such as unsecured modem access in legacy SCADA systems and known weaknesses in **Remote Terminal Units (RTUs)**.

To manage these risks, organizations can utilize frameworks such **as the NIST Cybersecurity Framework (CSF)** and **MITRE ATT&CK**. Effective controls include the deployment of **End-to-End Encryption (E2EE)** between RTUs and SCADA systems (preventive) and continuous **network traffic monitoring** (detective). Best practices for incident response include the establishment of a **Computer Security Incident Response Team (CSIRT)** and the implementation of network segmentation. The urgency of these measures is underscored by recent geopolitical incidents, including drone attacks on the Zaporizhzhia plant in Ukraine and physical strikes on Iranian nuclear facilities.

2 Sectors

2.1 Critical Infrastructure Sector

The "Nuclear Reactors, Materials, and Waste" sector and its accompanying organizations operate reactors [4] that generate energy and materials utilized in medical, agricultural, and other commercial uses [25].

The scope of this work from this sector yields tremendous economic and environmental benefits to the nation while protecting the safety of employees and social relationships [24]. The sector's mission aligns with the national security mission involving economic stability and public safety [16].

2.2 Organizations

The Nuclear Regulatory Commission (NRC) is an independent US agency that works to improve the safety and security of nuclear reactor sites and surrounding areas [23]. NRC has strict procedures and steps set to support the organizations in treating waste while protecting their revenue-generating operations, which overall improves the national security mission to protect public safety.

The Department of Energy is a US federal agency that conducts research and development to improve methods of nuclear energy and material production [17]. These technological breakthroughs are implemented to an organization's operations, in order to improve revenue-generating output, which also aids the national security mission to improve economic stability [16].

2.3 Assets

One asset that is of the "high" critical nature is the physical infrastructure of the nuclear reactors themselves. In absence of the physical infrastructure, nuclear energy cannot be produced without destructive consequences - the production of energy and materials would be obsolete for the organization [15]. The physical infrastructure yields various products, which ultimately produces economic and environmental benefits from within the sector.

An asset that leans within the "medium" tier on the criticality scale would be the intellectual property and classified information produced at the nuclear reactors for the purpose of commercializing such materials [8]. IP permits organizations to efficiently innovate ways to produce nuclear energy and materials. This would aid the sector overall in not only contributing to the output, but also in innovative ways of safely doing so [19].

2.4 Security Regulations

The NRC lays out in its Code of Federal Regulation, the following: § 73.27(b) requires licensee who receive a shipment of nuclear materials to urgently notify the delivery carrier, the Director, Division of Physical and Cyber Security Policy, and the Office of Nuclear Security and Incident Response to confirm the receival of delivery [21]. The involvement of all the parties function to ensure live-time oversight of material delivery which helps assure security, potentially to prevent malicious actors from obtaining highly toxic and well-researched materials.

In the same document, § 73.54(d)(2) states the required responsibility of organizations to adequately train their employees and contractors regarding cyber security requirements and practices that revolve around their core job performance functions [22].

2.5 Threats

One looming and potential threat lies upon the dependence on distributed control systems (DCS) within a nuclear facility [9]. Market available security solutions are difficult to implement because of the nature of the rigidity, control, and sensitivity of the systems and information encompassing the nuclear sector.

Another potential threat is insider threat, directed and operated either intentionally or unintentionally by the people working for the organizations in this sector. While not always intentional, the product of an internal assault can have dire consequences [18].

2.6 Threat Intelligence Sources

One tremendously beneficial source for threat intelligence for the selected sector would be the alerts and advisories compiled by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) [20]. CISA provides live updates and potential vulnerabilities intelligence applicable to the sector, often sourcing accurate information like foreign governments and other trust sources.

Another source for threat intelligence is MITRE ATT&CK, which retains a repository of adversarial techniques and practices [11].

Organizations could jointly utilize CISA's alerts and reference MITRE's sources to understand threat actors and the processes that they use to operate.

2.7 Frameworks

A potential framework that can be utilized is the CSF Framework from the National Institute of Standards & Technology (NIST) [12]. This framework is intended to assist organizations in understanding and mitigating cybersecurity risks.

Another framework organizations in this sector could utilize would be the MITRE ATT&CK Framework which categorizes an adversary's common behaviors.

2.8 Vulnerabilities

A known vulnerability exists within the remote terminal units (RTUs) [5] that are used in SCADA systems and devices. RTUs are data and control concentrators, usually feeding information to programmable logic controllers (PLCs) [1].

Another known vulnerability still exists regarding unsecured modem access within SCADA systems and devices [9]. Many older organizations may have legacy systems with outdated modems or the cost associated with carrying out replacements were considered too expensive.

2.9 Controls

One preventative control that the organization could deploy in this sector would be to create an end to end encryption (E2EE) method between the RTUs and PLCs or the SCADA system as a whole [6].

A detective control that the organization could deploy would be to continuously monitor network traffic by logging network traffic for further analysis [13].

2.10 Incident Response Best Practices

One good practice would be to create a Computer Security Incident Response Team (CSIRT), which is a specific incident team that utilizes a cybersecurity policy framework to address cyber incidents [7].

With the newfound CSIRT, another good practice would be for the team to segment their network in order to limit and isolate the spread of a breach in the case of a cyber attack [3].

2.11 Recent Incidents

On June 5th, 2025, the recently Russian occupied Zaporizhzhia plant in Ukraine was physically attacked by gunfire set off using drones [14].

On June 21st, 2025, the US military struck 3 Iranian nuclear facilities known as the Fordow Uranium Enrichment Plant, the Natanz Nuclear Facility, and the Isfahan Nuclear Technology Center [2].

On April 28th, 2025, there were large power outages in Spain and Portugal - potentially inferred to be from a cyberattack according to Spain's National Institute for Cybersecurity (INCIBE) [10].

[1] Ayodeji, Abiodun., et al. "Cyber security in the nuclear industry: A closer look at digital control systems, networks and human factors." sciencedirect.com, www.sciencedirect.com/science/article/pii/S0149197023001737. Accessed 12 Sept. 2025.

[2] Baev, Pavel K., et al. "The Global Implications of the US Strikes on Iran." Brookings, 2 July 2025, www.brookings.edu/articles/the-global-implications-of-the-us-strikes-on-iran/. Accessed 12 Sept. 2025.

[3] CompTIA. "What Is Network Segmentation and Why Does It Matter?" *Information Technology (IT) Certifications & Tech Training | CompTIA*, www.comptia.org/en-us/blog/what-is-network-segmentation-and-why-does-it-matter/. Accessed 12 Sept. 2025.

[4] Cybersecurity & Infrastructure Security Agency. "Nuclear Reactors, Materials, and Waste Sector." *CISA*, www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/nuclear-reactors-materials-and-waste-sector. Accessed 12 Sept. 2025.

[5] Hitachi. "Hitachi Energy's RTU Cybersecurity Solutions Deliver Peace of Mind." Hitachi Energy - Inspire the Next Era of Sustainable Energy, www.hitachienergy.com/news-and-events/customer-stories/abb-s-rtu-cyber-security-solutions-deliver-peace-of-mind. Accessed 12 Sept. 2025.

[6] IBM. "What Is End-to-End Encryption?" *IBM - United States*, www.ibm.com/think/topics/end-to-end-encryption. Accessed 12 Sept. 2025.

[7] International Atomic Energy Agency. "Computer Security Incident Response Planning at Nuclear Facilities." Pub.IAEA.org, www-pub.iaea.org/MTCD/Publications/PDF/TDL005web.pdf. Accessed 12 Sept. 2025.

[8] Buchan, James H., "The Role of Intellectual Property in the Nuclear Sector." GOWLING WLG, 7 Aug. 2025, gowlingwlg.com/en/insights-resources/articles/2025/ip-in-the-nuclear-sector. Accessed 12 Sept. 2025.

[9] Hieb, Jeff., "Security hardened remote terminal units for SCADA networks." ThinkIR: The University of Louisville's Institutional Repository, University of Louisville, ir.library.louisville.edu/cgi/viewcontent.cgi?article=1614&context=etd. Accessed 12 Sept. 2025.

[10] McCallion, Jane. "Blackouts in Spain and Portugal Could Be a Cyber Attack." IT Pro, 28 Apr. 2025, www.itpro.com/security/cyber-attacks/blackouts-in-spain-and-portugal-could-be-a-cyber-attack. Accessed 12 Sept. 2025.

[11] MITRE | ATT&CK®. "Get Started." MITRE ATT&CK®, attack.mitre.org/resources/. Accessed 12 Sept. 2025.

[12] National Institute of Standards and Technology. "The NIST Cybersecurity Framework (CSF) 2.0." NIST Technical Series Publications, U.S. Department of Commerce, nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf. Accessed 12 Sept. 2025.

[13] Palo Alto Tech Docs. "What Data Center Traffic to Log and Monitor." Palo Alto Networks | TechDocs Home, docs.paloaltonetworks.com/best-practices/10-2/data-center-best-practices/data-center-best-practice-security-policy/log-and-monitor-data-center-traffic/what-data-center-traffic-to-log-and-monitor.Accessed 12 Sept. 2025.

[14] Reuters. "IAEA team at Ukraine's Zaporizhzhia says it heard repeated rounds of gunfire." Reuters.com, www.reuters.com/world/europe/iaea-team-ukraines-zaporizhzhia-says-it-heard-repeated-rounds-gunfire-2025-06-05/?utm_source=chatgpt.com. Accessed 12 Sept. 2025.

[15] Synapse Energy Economics, Inc. "Nuclear Power Plant Construction Costs." Synapse Energy, www.synapse-energy.com/sites/default/files/SynapsePaper.2008-07.0.Nuclear-Plant-Construction-Costs.A0022_0.pdf. Accessed 12 Sept. 2025.

[16] U.S. Department of Energy. "Stakeholder Outreach." Energy.gov, www.energy.gov/pppo/stakeholder-outreach. Accessed 12 Sept. 2025.

[17] ---. "3 Surprising Ways to Use Nuclear Energy." Energy.gov, www.energy.gov/ne/articles/3-surprising-ways-use-nuclear-energy. Accessed 12 Sept. 2025.

[18] U.S. Government Publishing Office. "- SECURING THE MODERN ELECTRIC GRID FROM PHYSICAL AND CYBER ATTACKS." GovInfo | U.S. Government Publishing Office, www.govinfo.gov/content/pkg/CHRG-111hhrg53425/html/CHRG-111hhrg53425.htm. Accessed 12 Sept. 2025.

[19] U.S. Homeland Security. "National Infrastructure Protection Plan." Homeland Security, www.dhs.gov/xlibrary/assets/nipp_nuclear.pdf. Accessed 12 Sept. 2025.

[20] ---. "Nuclear Reactors, Materials, and Waste Sector-Specific Plan." CISA, www.cisa.gov/sites/default/files/publications/nipp-ssp-nuclear-2015-508.pdf. Accessed 12 Sept. 2025.

[21] U.S. Nuclear Regulatory Commission. "§ 73.27 Notification requirements." NRC.gov, www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0027.html. Accessed 12 Sept. 2025.

[22] ---. "§ 73.54 Protection of digital computer and communication systems and networks." NRC.gov, www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html. Accessed 12 Sept. 2025.

[23] ---. "About NRC." *nrc.gov*, www.nrc.gov/about-nrc. Accessed 12 Sept. 2025.

[24] World Nuclear Association. "Economics of Nuclear Power." World Nuclear Association, world-nuclear.org/information-library/economic-aspects/economics-of-nuclear-power. Accessed 12 Sept. 2025.

[25] ---. "The Many Uses of Nuclear Technology." World Nuclear Association, world-nuclear.org/information-library/non-power-nuclear-applications/overview/the-many-uses-of-nuclear-technology. Accessed 12 Sept. 2025.