VCDNP Vienna Center for Disarmament and Non-Proliferation

January 2026

Data Security Challenges in the Integration of IIoT and AI in the Nuclear Industry

Dr. Khalil El-Khatib
Dr. Pooria Madani

Vienna Center for Disarmament and Non-Proliferation | vcdnp.org

Authors

Dr. Khalil El-Khatib is a professor in Information Security at Ontario Tech University. His research interests include big data and security analytics, smart grid security, and cloud computing. He previously served as an Assistant Professor at the University of Western Ontario. He holds a PhD from the University of Ottawa and a graduate degree in Computer Science from McGill University.

Dr. Pooria Madani is an Assistant Professor of Business and Information Technology at Ontario Tech University. His research interests include adversarial machine learning, security of IoT, and Aerospace Security. He holds a PhD in Computer Science from York University and a graduate degree in Computer Science from the University of New Brunswick.

About the VCDNP

The Vienna Center for Disarmament and Non-Proliferation (VCDNP) promotes international peace and security by conducting research, facilitating dialogue, and building capacity on nuclear non-proliferation and disarmament.

The VCDNP is an international non-governmental organisation, established in 2010 by the Federal Ministry for European and International Affairs of Austria and the James Martin Center for Nonproliferation Studies at the Middlebury Institute of International Studies at Monterey.

Our research and analysis provide policy recommendations for decision-makers. We host public events and facilitate constructive, results-oriented dialogue among governments, multilateral institutions, and civil society. Through in-person courses and online resources on nuclear non-proliferation and disarmament, we train diplomats and practitioners working in Vienna and around the world.

Acknowledgements

This research and paper were made possible through the support of the Vienna Center for Disarmament and Non-Proliferation (VCDNP) as well as a research project funded by **Global Affairs Canada**.

VCDNP
Vienna Center for Disarmament and Non-Proliferation

Andromeda Tower, 13/1
Donau-City-Strasse 6
1220 Vienna
Austria

vcdnp.org
info@vcdnp.org
@VCDNP
VCDNP

Sponsored by
Canada

Contents

The Industrial Internet of Things has already resulted in efficiency and safety gains in traditional sectors like manufacturing and logistics.

Introduction

Industry 4.0 refers to the ongoing transformation of industry through the integration of cyber-physical systems, pervasive connectivity, and intelligent automation. At its core, it builds on technologies such as the Industrial Internet of Things (IIoT), where networks of sensors and devices generate vast amounts of real-time operational data, and artificial intelligence (AI), which leverages this data to enable AI-enhanced applications like predictive maintenance, anomaly detection, optimisation, and adaptive decision-making. According to the National Institute of Standards and Technology, IIoT is defined as "sensors, instruments, machines, and other devices that are networked together and use Internet connectivity to enhance industrial and manufacturing business processes and applications."[1] In traditional sectors like manufacturing and logistics, Industry 4.0 technologies have resulted in substantial improvements in efficiency, reduced downtime, streamlined supply chains, and enhanced safety oversight.

Nuclear energy – though historically conservative in adopting new digital technologies due in large part to strict regulatory and safety requirements – is not immune to the broader pressures leading other sectors to adapt Industry 4.0. Operators face demands to reduce costs, improve predictive safety analytics, and demonstrate resilience in an era of digital transformation. The promise of Industry 4.0 for the nuclear sector lies in its ability to support early fault detection, smarter maintenance cycles, and enhanced data-driven oversight leading to reduced costs, improved safety analytics, and optimised work operations.

1 Ron Ross et al., "Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171," NIST SP 800-172, U.S. Department of Commerce, February 2021, p. 42. Available at: https://doi.org/10.6028/NIST.SP.800-172.

IIoT typically extends the range of interconnectivity in traditional Supervisory Control and Data Acquisition (SCADA) systems by using various wireless technologies, including Bluetooth, Wi-Fi, cellular, low-power wide area network, and satellite communications. It is important to highlight that IIoT systems are not expected to replace traditional SCADA systems but rather to enhance their capabilities through data collection and data analytics. Data collected from various strategically deployed sensors (vibration, radiation, temperature, humidity, pressure sensors), combined with various AI and machine learning algorithms that process this data in new ways, can prove to be revolutionary.

The benefits of IIoT for the nuclear sector are less clear than for other sectors, like logistics and manufacturing. Nuclear plants rely on highly reliable SCADA and operational technology (OT) systems with stringent redundancies. Additional IIoT sensors may offer only marginal benefits while introducing regulatory burdens, lifecycle validation challenges, and potentially significant cyber risks. This raises the question: do IIoT's promised gains of real-time analytics and predictive maintenance justify the risks in a safety-critical sector where reliability and compliance outweigh efficiency?

This paper critically examines the implications of adopting Industry 4.0 technologies – specifically IIoT and AI – within the nuclear sector. It begins by outlining how the introduction of IIoT devices expands the attack surface, introducing new technical, supply chain, and physical security vulnerabilities. The paper then analyses the risks to data integrity and operational reliability, with particular attention to adversarial manipulation, data poisoning, and cascading effects across interconnected systems. Building on this, the paper will discuss threats specific to AI models themselves, including model inversion, theft, trojaning, and system hijacking, all of which present novel vectors of exploitation. The paper further explores gaps in governance, compliance, and ethical frameworks that complicate the safe adoption of these technologies in the nuclear domain. Finally, it will reflect on the strategic paradox facing nuclear operators: balancing pressures for modernisation with the uncompromising need for safety, security, and reliability.

IIoT paired with AI could be both beneficial to nuclear operations and expand the potential attack surface.

Threat Analysis for Integrating IIoT in the Nuclear Sector

In nuclear operations, IIoT technologies primarily serve as a data-collection backbone, generating massive volumes of real-time sensor and telemetry data from reactors, turbines, cooling systems, and auxiliary equipment. On their own, these raw data streams are too vast and complex to be interpreted manually or even through conventional rule-based systems. When paired with AI and machine learning techniques, however, the value of this data becomes immense.

These techniques can filter, contextualise, and act on the data, enabling applications from anomaly detection and predictive maintenance to automated safety decision-support. This interdependence means that IIoT and AI cannot be considered in isolation: without AI, IIoT devices risk becoming “data exhaust”, while without trusted IIoT data, AI models are left blind or misinformed. The result is an increasingly semi- to fully-automated system of layered architecture, where AI provides an enhanced data processing/analytic layer atop IIoT’s sensing layer, amplifying both the operational benefits and the potential attack surface in nuclear Industry 4.0 environments.

Integrating IIoT technologies into the nuclear sector can offer significant advantages, e.g. real-time monitoring, predictive maintenance, increased efficiency, but their integration also increases the cyberattack surface and can introduce serious threats.[2,3,4]

Figure 1. Overview of IIoT and AI Specific Threats to the Nuclear Energy Sector

2 Michael Fagan et al., "Foundational Cybersecurity Activities for IoT Device Manufacturers", NIST, U.S. Department of Commerce, NISTIR 8259, May 2020. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf.

3 International Atomic Energy Agency, "Computer Security of Instrumentation and Control Systems at Nuclear Facilities", IAEA Nuclear Security Series, No. 33-T, 2018. Available at: https://www-pub.iaea.org/MTCD/Publications/PDF/P1787_web.pdf.

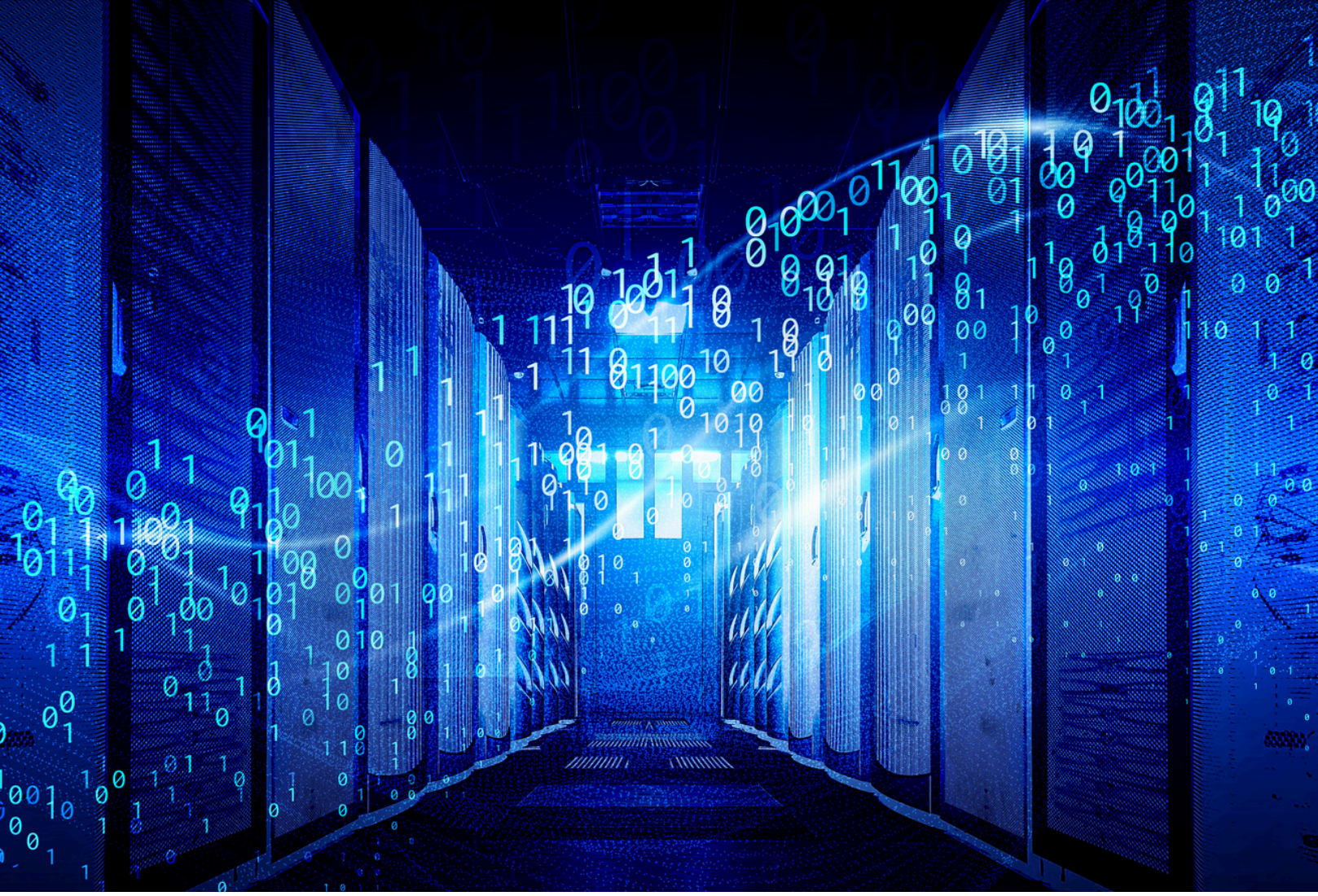
4 Jibran Saleem et al., "IoT standardisation: challenges, perspectives and solution", Proceedings of the 2nd International Conference on Future Networks and Distributed Systems, Art. No. 1, pp. 1–9, 26 Jun 2018. Available at: https://doi.org/10.1145/3231053.3231103.

Supply chain risk represents another significant concern, particularly if systems' owners deploy off-the-shelf devices without proper evaluation of the Bill-of-Materials for these devices.[5,6] Many IIoT devices, hardware or software, may contain vulnerabilities (embedded maliciously or unintentionally) introduced by a third-party. In addition, IIoT devices can introduce further vulnerabilities if they were produced by vendors with poor security practices, for example hardcoding credentials where sensitive information like usernames, passwords, or tokens are directly written into the source code. Furthermore, if validation protocols are too strict it might result in devices not receiving timely security updates.

The integration of IIoT into nuclear operations risks reducing human oversight, increasing dependence on devices that may themselves be vulnerable. In contrast to conventional SCADA and OT systems, IIoT systems demand regular updates, remote management, and often consist of devices supplied by multiple vendors. This shift not only introduces cyber risk but also elevates the importance of the physical security of devices – if sensors are tampered with or physically replaced, the resulting data manipulation may directly misguide AI-driven decision-making. Moreover, the diversity of vendors in IIoT ecosystems often clashes with the nuclear sector's emphasis on consistency and compliance, amplifying risks, such as those associated with patch delays (e.g. one vendor may rapidly release security updates while another delays patches due to certification requirements, leaving parts of the system exposed), weak security practices, or compromised supply chains.

5 Shannon Leigh Eggers, "The Nuclear Digital I&C System Supply Chain Cyber-Attack Surface", Idaho National Laboratory, June 2020. Available at: https://www.osti.gov/servlets/purl/1634821.

6 Shannon Leigh Eggers and Michael Rowland, "Deconstructing the Nuclear Supply Chain Cyber-Attack Surface", Idaho National Laboratory, July 2020. Available at: https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_26002.pdf.



Bad actors could exploit IIoT in nuclear facilities by manipulating input data, e.g. to lower the reported temperature or pressure values inside a containment system during an emergency.

Operation of Nuclear Systems under Adversarial Input Data

One of the most pressing concerns when integrating IIoT and AI into nuclear operations is the assurance of data integrity. Unlike in many other industrial environments where errors can be tolerated, even minor deviations in nuclear data (e.g. false data) can lead to disproportionate consequences on the action taken. Nuclear operations rely heavily on precise sensor measurements – radiation levels, coolant flow rates, vibration readings from pumps and turbines, or containment pressure levels – to ensure safety, compliance, and operational continuity. A single maliciously manipulated sensor feed can trigger inappropriate automated responses, disrupt critical safety functions, or mislead operators during crisis scenarios.[7]

For instance, consider a scenario where an attacker subtly lowers the reported temperature or pressure values inside a containment system during an emergency. If the control room receives falsified readings that appear "within normal limits", operators may delay activating emergency cooling or ventilation systems. Meanwhile, the real temperature or pressure continues to rise unchecked, narrowing the time window for safe intervention. In a more automated setup, an AI-driven system trained on corrupted data may fail to recognise the anomaly entirely, suppress alarms, or recommend an inappropriate response – turning what should have been a contained incident into a cascading systems failure.

7 Michael Fagan et al., "Foundational Cybersecurity Activities for IoT Device Manufacturers", NIST, U.S. Department of Commerce, NISTIR 8259, May 2020. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf.

Adversaries are motivated to target data integrity because of the potential strategic and economic impact. For example, injecting falsified high-vibration readings from turbine sensors could force an unnecessary emergency reactor scram, resulting in significant financial loss and reputational damage without requiring physical intrusion.[8] Conversely, suppressing real anomaly signals – such as masking coolant pump degradation – could buy time for adversaries to escalate an attack or cause the system to drift toward unsafe conditions.[9] Both scenarios undermine operator trust in monitoring systems, trust which is critical in high-risk nuclear settings.

The use of AI-driven predictive maintenance and anomaly detection introduces new categories of risks in the form of adversarial machine learning inputs. As Makhzani et al. demonstrated, carefully crafted adversarial examples can mislead AI models into producing incorrect classifications while appearing benign to humans.[10] In nuclear operations, adversarial perturbations to radiation or vibration sensor data could cause anomaly detectors to misclassify dangerous conditions as normal, delaying corrective action.[11] Such an attack may be driven by motives ranging from causing disruption and confusion to concealing intentional acts of sabotage.

Equally concerning are data poisoning attacks, where the training data for predictive models is corrupted. Biggio et al.[12] and Steinhardt et al.[13] showed how attackers can inject carefully selected malicious samples into training datasets to embed long-lasting vulnerabilities in machine learning models. In the nuclear context, data poisoning could occur if IIoT logs or vendor-supplied maintenance data are manipulated for example, before model training. A poisoned predictive model might "learn" to treat early fault signatures as benign, effectively blinding operators to critical equipment degradation.[14] Unlike one-time manipulations, poisoning has a persistent and systemic effect.

In the nuclear sector, these risks are amplified due to the cascading interdependencies of its systems. An integrity breach in a single subsystem (e.g. coolant flow monitoring) may propagate across interconnected dashboards, predictive algorithms, and automated control loops. This creates confusion during operations and undermines forensic investigations after an incident, since manipulated data streams may obscure the root cause.[15] In such high-consequence environments, adversarial inputs and data manipulation represent not just cyber risks, but direct challenges to nuclear safety and regulatory compliance.

8 Jibran Saleem et al., "IoT standardisation: challenges, perspectives and solution", Proceedings of the 2nd International Conference on Future Networks and Distributed Systems, Art. No. 1, 26 Jun 2018, pp. 1–9. Available at: https://doi.org/10.1145/3231053.3231103.

9 International Atomic Energy Agency, "Computer Security of Instrumentation and Control Systems at Nuclear Facilities", IAEA Nuclear Security Series, No. 33-T, 2018. Available at: https://www-pub.iaea.org/MTCD/Publications/PDF/P1787_web.pdf.

10 Alireza Makhzani et al., "Adversarial Autoencoders", arXiv preprint arXiv:1511.05644, 25 May 2016. Available at: https://arxiv.org/pdf/1511.05644.

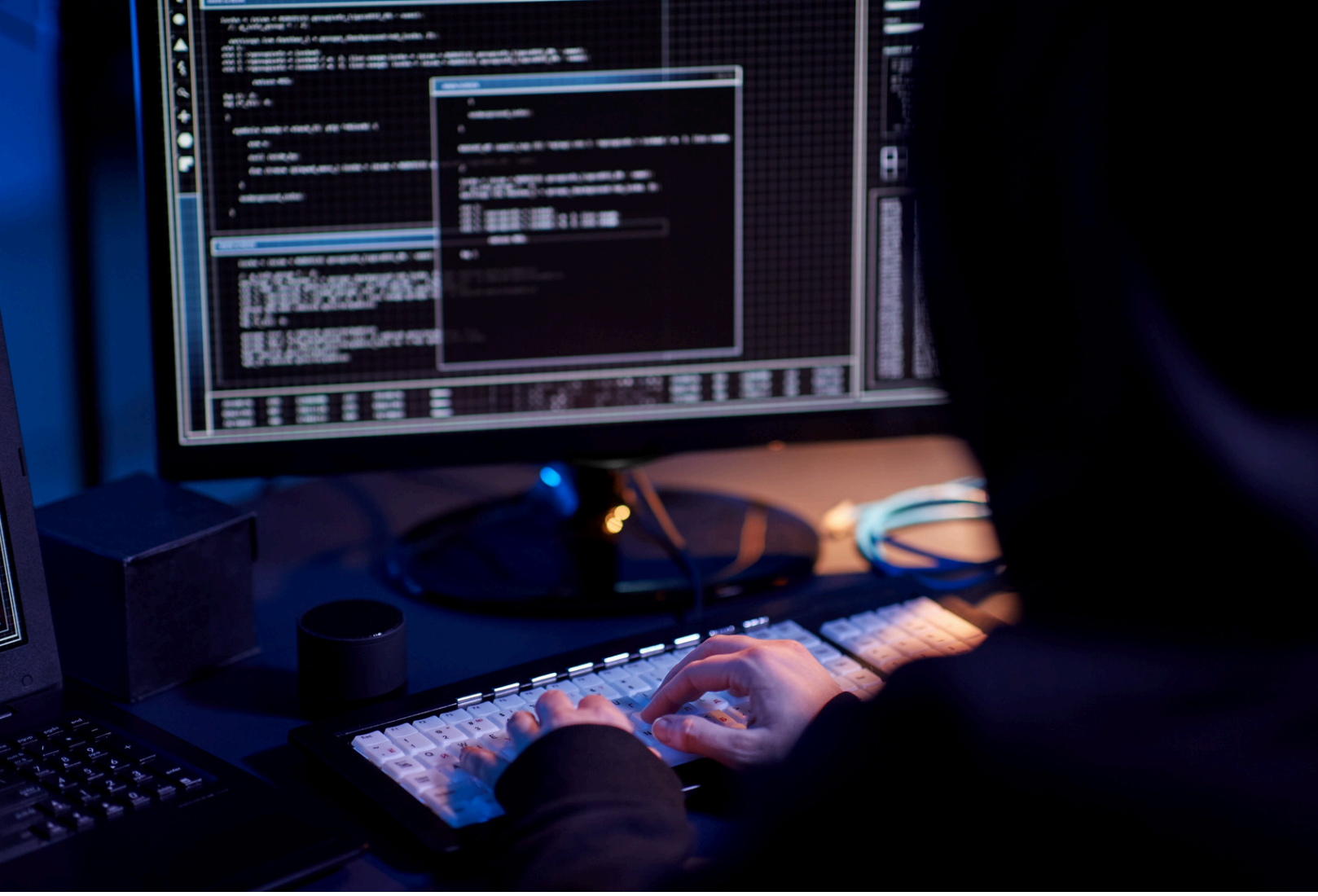
11 International Atomic Energy Agency, "Artificial Intelligence for Accelerating Nuclear Applications, Science and Technology", IAEA Scientific and Technical Publication, 2022. Available at: https://www-pub.iaea.org/MTCD/Publications/PDF/ART-INTweb.pdf.

12 Battista Biggo et al., "Poisoning Attacks against Support Vector Machines", arXiv preprint arXiv:1206.6389, 25 Mar 2013. Available at: https://arxiv.org/pdf/1206.6389.

13 Jacob Steinhardt, Pang Wei Koh, and Percy Liang, "Certified Defenses for Data Poisoning Attacks", 31st Conference on Neural Information Processing Systems, 2017. Available at: https://proceedings.neurips.cc/paper_files/paper/2017/file/9d7311ba459f9e45ed746755a32dcd11-Paper.pdf.

14 International Atomic Energy Agency, "Life Cycle Management Approaches for Nuclear Facility Instrumentation and Control Systems", IAEA Nuclear Energy Series, No. NR-T-1.23, 2025. Available at: https://www-pub.iaea.org/MTCD/publications/PDF/p15653-PUB2100_web.pdf.

15 Ibid.



Malicious actors could uncover sensitive information about nuclear facilities through attacks on AI systems used in such facilities.

AI Model Exploitation

Beyond the manipulation of IIoT sensor data, the AI models themselves represent high-value attack surfaces when deployed in nuclear facilities. These models – ranging from anomaly detectors to decision-support systems – encode sensitive operational knowledge and can be exploited by adversaries seeking to conduct espionage, or sabotage, or for strategic leverage.[16]

One pathway is model inversion, where attackers query an AI system and reconstruct sensitive features of the training data. Fredrikson et al.[17] demonstrated how inversion attacks can expose hidden attributes from machine learning models, while Shokri et al.[18] extended this to membership inference attacks, showing how adversaries can determine if specific data records were part of a training set. In the nuclear context, such leakage could reveal operational rhythms, reactor load profiles, or equipment degradation patterns, which may otherwise be classified or restricted information.[19]

16 International Atomic Energy Agency, “Artificial Intelligence for Accelerating Nuclear Applications, Science and Technology”, IAEA Scientific and Technical Publication, 2022. Available at: https://www-pub.iaea.org/MTCD/Publications/PDF/ART-INTweb.pdf.

17 Matt Fredrikson, Somesh Jha, and Thomas Ristenpart, "Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures", In Proceedings of the 22nd ACM SIGSAC conference on computer and communications security, pp. 1322-1333,12 Oct 2015. Available at: https://dl.acm.org/doi/pdf/10.1145/2810103.2813677.

18 Reza Shokri et al., "Membership Inference Attacks Against Machine Learning Models", In 2017 IEEE Symposium on Security and Privacy (SP), IEEE, 2017, pp. 3-18. Available at: https://www.computer.org/csdl/proceedings-article/sp/2017/07958568/12OmNBUAvVc.

19 International Atomic Energy Agency, “Computer Security of Instrumentation and Control Systems at Nuclear Facilities”, IAEA Nuclear Security Series, No. 33-T, 2018. Available at: https://www-pub.iaea.org/MTCD/Publications/PDF/P1787_web.pdf.

Another risk is model theft and replication. Tramèr et al. demonstrated how adversaries can extract a target model's decision boundaries by repeated queries, allowing them to build a functionally equivalent copy.[20] Applied to nuclear anomaly detection models, theft enables attackers to test manipulations offline until they find consistent blind spots, which can then be exploited against live systems.[21] This ability to study and probe a model outside the secure facility environment increases the likelihood of successful undetected attacks.

Even more concerning is the possibility of backdoored or trojaned AI models. Gu et al. showed how malicious actors can embed hidden triggers into AI models that remain dormant under normal conditions but activate under specific, rare inputs.[22] In nuclear contexts, a trojaned vendor-supplied AI model might suppress safety alarms only when vibration exceeds a particular threshold or when multiple sensors simultaneously register specific values. Given the reliance on external vendors, contractors, and open-source models in many IIoT deployments, this supply chain risk is non-trivial.[23]

While it is true that many nuclear facilities or critical infrastructure operators deploy customised or closed-source AI systems, it is important to recognise how these are commonly developed in practice. Modern generative and large-scale AI models are prohibitively expensive to train from scratch, requiring access to vast datasets, large-scale compute clusters, and highly specialised expertise. As a result, even in highly regulated domains such as nuclear safety, the field is moving toward relying on existing base models – often open-source models released by academic institutions or major AI labs – and then applying domain-specific fine-tuning or transfer learning to adapt them for operational use.

This development pipeline has two important implications for supply chain security. First, the "custom" or "closed" nature of the final model does not eliminate dependence on the integrity of the original base model. If a foundational model is compromised (e.g. via backdoor insertion or training data poisoning) those malicious behaviours can persist and remain embedded even after fine-tuning. Second, because fine-tuning generally adjusts weights without fully retraining the network, it is unlikely to erase subtle triggers or dormant behaviours intentionally implanted in the base model. Therefore, any downstream system, no matter how specialised or closed, can inherit these risks. In the context of IIoT devices deployed in nuclear facilities, this underscores that making choices for systems to integrate between open-source, closed-source, and customised models on the basis of security is not cleanly protective. The supply chain remains exposed wherever foundational dependencies exist, making rigorous provenance checks, model auditing, and adversarial testing essential.

Finally, system hijacking represents the most severe AI-specific threat. If adversaries gain control of the AI decision logic itself, they could gradually degrade reactor safety margins by altering setpoints, suppressing anomaly alerts, or rescheduling maintenance in ways that increase risk. Such manipulations pose significant limitations and risks in the nuclear domain because of the explainability gap inherent in contemporary AI models and systems – as is the case with deep learning models that frequently deliver accurate results without offering clear reasoning, which hampers operators' ability to critically assess the outputs. Regulatory guidance such as those published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) (e.g. ISO/IEC 42001) emphasises explainability and trust in AI governance but gaps remain, particularly in high-stakes nuclear applications where opaque recommendations may be wrongly accepted.[24]

20 Florian Tramèr et al., "Stealing Machine Learning Models via Prediction APIs", In 25th USENIX Security Symposium, Aug 2016, pp. 601-618. Available at: https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_tramer.pdf.

21 Jibran Saleem et al., "IoT standardisation: challenges, perspectives and solution", Proceedings of the 2nd International Conference on Future Networks and Distributed Systems, Art. No. 1, 26 Jun 2018, pp. 1–9. Available at: https://doi.org/10.1145/3231053.3231103.

22 Tianyu Gu, Brendan Dolan-Gavitt, and Siddharth Garg, "BadNets: Identifying Vulnerabilities in the Machine Learning Model Supply Chain", arXiv preprint arXiv:1708.06733, 11 Mar 2019. Available at: https://arxiv.org/pdf/1708.06733.

23 Michael Fagan et al., "Foundational Cybersecurity Activities for IoT Device Manufacturers", NIST, U.S. Department of Commerce, NISTIR 8259, May 2020. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf.

24 Elodie Broussard, "The Future of Atoms: Artificial Intelligence for Nuclear Applications", IAEA Bulletin, Vol. 61, No. 4, Nov. 2020, pp. 34–35. Available at: https://www.iaea.org/bulletin/the-future-of-atoms-artificial-intelligence-for-nuclear-applications.

AI systems in nuclear environments can be exploited by attackers through various techniques. Espionage-driven actors may seek sensitive operational intelligence through inversion and membership inference.[25] Economic and other adversaries may trigger costly reactor shutdowns by feeding adversarial inputs into predictive maintenance models.[26] Saboteurs with a range of aims may seek to introduce backdoored models to degrade nuclear safety while avoiding detection.[27] Other malicious actors may exploit AI hijacking capabilities as a form of strategic deterrence or coercion.[28]

These risks demand tailored AI assurance strategies for nuclear facilities. For example, defences may include adversarial training to harden models against crafted inputs,[29] runtime monitoring to detect anomalous model behaviour, strict supply-chain vetting of externally sourced AI, and hybrid human–machine oversight mechanisms where operator expertise complements automated decision-making. Without such measures, IIoT devices, especially when enhanced by AI, risk introducing new vulnerabilities at the core of nuclear facility systems.

25 International Atomic Energy Agency, “Computer Security of Instrumentation and Control Systems at Nuclear Facilities”, IAEA Nuclear Security Series, No. 33-T, 2018. Available at: https://www-pub.iaea.org/MTCD/Publications/PDF/P1787_web.pdf.

26 Jibran Saleem et al., “IoT standardisation: challenges, perspectives and solution”, Proceedings of the 2nd International Conference on Future Networks and Distributed Systems, Art. No. 1, 26 Jun 2018, pp. 1–9. Available at: https://doi.org/10.1145/3231053.3231103.

27 Reza Shokri et al., "Membership Inference Attacks Against Machine Learning Models", In 2017 IEEE Symposium on Security and Privacy (SP),IEEE, 2017, pp. 3-18. Available at: https://www.computer.org/csdl/proceedings-article/sp/2017/07958568/12OmNBUAvVc.

28 Elodie Broussard, “The Future of Atoms: Artificial Intelligence for Nuclear Applications”, IAEA Bulletin, Vol. 61, No. 4, Nov. 2020, pp. 34–35. Available at: https://www.iaea.org/bulletin/the-future-of-atoms-artificial-intelligence-for-nuclear-applications.

29 Alexey Kurakin, Ian J. Goodfellow, and Samy Bengio, "Adversarial Machine Learning at Scale", arXiv preprint arXiv:1611.01236, 11 Feb 2017. Available at: https://arxiv.org/pdf/1611.01236.

The integration of IIoT and AI in nuclear facilities could introduce data governance, compliance, standardisation, and ethical concerns.

Data Governance and Standards

Adopting AI and IIoT in the nuclear sector may bring transformative potential – improving operational efficiency, safety, and predictive maintenance. AI technologies can process vast amounts of data to "learn" how to perform specific tasks. However, their use also introduces a complex set of data governance, compliance, standardisation, and ethical concerns, due to the sensitive, high-risk nature of nuclear infrastructure.

Today, there is no industry-accepted and efficient method for tracking the usage characteristics of IIoT systems data and devices, whether they are connected via the cloud or locally. Unlike data used by SCADA systems, data generated by IIoT systems can be labelled as classified, sensitive, operational, and non-sensitive data.[30] The nuclear sector is starting to adopt integrated product lifecycle management solutions to ensure data flows seamlessly from design to operation.[31] These solutions often rely on the ISO 15926 for integrating, exchanging, and transferring data across different systems.[32] Nonetheless, challenges can arise regarding data ownership, as it is frequently ambiguous who holds the legal rights to the data produced by IIoT devices and/or outputs generated by AI models that ingest this data, especially within operational management settings.

30 How IIoT data is labelled will vary from one country to another, based on local regulations, standards and compliance requirements.

31 Jingli Ren and Pan Yang, "Lifecycle Data Management of Nuclear Power Plant: Framework System and Development Suggestions", Strategic Study of CAE, Vol. 24, No. 2, 2022, pp. 152-159. Available at: https://www.engineering.org.cn/sscae/EN/10.15302/J-SSCAE-2022.02.012.

32 International Organization for Standardization, “Industrial Automation Systems and Integration — Integration of Life-Cycle Data for Process Plants Including Oil and Gas Production Facilities”, Part 2: Data Model, ISO 15926-2:2003, 2003. Available at: https://www.iso.org/standard/29557.html.

Additionally, data and data-inferred lifecycle management still lack a [common] definition. While a recent 2025 International Atomic Energy Agency (IAEA) publication on "Life Cycle Management Approaches for Nuclear Facility Instrumentation and Control [I&C] Systems" offers guidance on lifecycle management of I&C systems, with relevance to design, development, operation, maintenance, verification, validation, and decommissioning – it is not IIoT data-specific and might be very constrained for IIoT data.[33]

The IEC 62443 framework is a related cybersecurity standard for industrial control systems, which helps to secure IIoT data flows, but not lifecycle management per se.[34] The framework provides a vendor-neutral, scalable, and comprehensive structure that supports regulatory compliance and reduces cyber risk in industrial environments which can be used for IIoT systems. In adopting the internationally recognised IEC 62443 framework, national governments, entities, and regulators could establish a harmonised baseline to support future regulatory compliance for cybersecurity controls in IIoT. The IEC is in the process of developing a technical specification to extend industrial cybersecurity principles to IIoT systems. Though it is still under development, the IEC 62443-1-6 technical specification, titled "Applying the 62443 Series to the Industrial Internet of Things (IIoT)" underscores recognition that IIoT brings unique cybersecurity considerations.[35]

The recently adopted EU Cyber Resilience Act, introduced EU-wide cybersecurity requirements for the design, development, and production of products with digital elements, including IIoT devices. The objective of the law is to improve the security of these products and to ensure transparency and compliance of producers.[36] Similarly, a standard from the Canadian Digital Governance Standards Institute (DGSI), the Cybersecurity of Industrial Internet of Things (IIoT) Devices (CAN/DGSI 105), established minimum requirements for IIoT systems with regards to security, confidentiality, integrity, availability, and safety. The framework includes strong data governance provisions and may influence broader energy-sector practices.

While no dedicated standard currently exists that specifically governs AI-driven IIoT in nuclear environments, there are a number of established frameworks and initiatives that could provide a relevant foundation for building up specific IIoT enhanced by AI devices standards going forward, including the ISO/IEC 42001:2023 AI Management System[37] and the US Nuclear Regulatory Commission AI Strategic Plan.[38] Another interesting governance framework is the AI Observatory that is proposing a governance model tailored for the nuclear sector.[39]

A further important aspect for integrating AI and IIoT into the nuclear sector is addressing ethical concerns. While eliminating redundancy and repetitive tasks is a key advantage of using AI, especially with the abundance of data to be processed, the key question becomes whether AI systems should be allowed to make autonomous decisions in safety-critical nuclear operations.[40]

33 International Atomic Energy Agency, "Life Cycle Management Approaches for Nuclear Facility Instrumentation and Control Systems", IAEA Nuclear Energy Series, No. NR-T-1.23, 2025. Available at: https://www-pub.iaea.org/MTCD/publications/PDF/p15653-PUB2100_web.pdf .

34 International Electrotechnical Commission, "System Security Requirements and Security Levels", Part 3-3, Technical Committee TC 65 Industrial-process measurement, control and automation, IEC 62443-3-3:2013, 2013.

35 Forthcoming International Electrotechnical Commission (IEC) technical standard: Applying the 62443 Series to the Industrial Internet of Things (IEC 62443-1-6).

36 Regulation (EU) 2024/2847, "Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)", Official Journal of the European Union, 20 Nov 2024. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402847.

37 International Organization for Standardization, "Information Technology — Artificial Intelligence — Management System", ISO/IEC 42001:2023, 2023.

38 United States Nuclear Regulatory Commission, "Artificial Intelligence Strategic Plan, Fiscal Years 2023 – 2027", NUREG-2261. Available at: https://www.nrc.gov/docs/ML2313/ML23132A305.pdf.

39 Anja Kaspersen and Wendall Wallach, "A Framework for the International Governance of AI", Carnegie Council for Ethics in International Affairs, 5 Jul 2023. Available at: https://carnegiecouncil.org/media/article/a-framework-for-the-international-governance-of-ai.

40 Canadian Nuclear Safety Commission, U.S. Nuclear Regulatory Commission, and Office for Nuclear Regulation, "Considerations for Developing Artificial Intelligence Systems in Nuclear Applications," September 2024. Available at: https://www.nrc.gov/docs/ML2424/ML24241A252.pdf.

An overreliance on AI may reduce operator engagement and critical thinking, and may completely bypass human judgment, leading to ethical risk in case of decisions that may have catastrophic consequences, raising the question of who would be responsible when an AI system makes an error. Discrimination is another concern, especially when AI systems are trained on biased data, which may produce unfair or unsafe outcomes, undermining trust in the system.

Finally, there is the question of transparency and explainability of AI models, particularly deep learning systems, which often lack interpretability. Most regulatory and safety standards adopted in the nuclear sector demand explainable decision-making to establish trust. Any AI system that makes decisions without providing justification undermines ethical standards of transparency, particularly in situations involving human life.

AI systems both benefit from and depend on the data richness of IIoT, yet this reliance creates novel vulnerabilities.

Conclusion

The integration of IIoT technologies and AI into nuclear operations presents both opportunities and challenges. While other sectors such as manufacturing, energy distribution, and logistics have adopted Industry 4.0 to drive efficiency, predictive maintenance, and cost reduction, the nuclear sector's core mission remains fundamentally different. Reliability, safety, and regulatory compliance take precedence over efficiency gains. Unlike consumer IoT or even conventional IIoT deployments, nuclear facilities already operate with sophisticated SCADA and OT systems designed for deterministic control and fault tolerance. In this context, the value proposition of IIoT must be weighed against its profound implications for data security, operational assurance, and lifecycle governance.

A recurring theme throughout this manuscript has been the expansion of the attack surface that accompanies IIoT and AI adoption. IIoT devices often rely on wireless connectivity, frequent updates, and diverse vendors, all of which run counter to the nuclear industry's emphasis on long-term stability and rigorous validation. The introduction of such devices does not only introduce cybersecurity risks, it also re-elevates physical security to the forefront, as tampered or sabotaged sensors can feed falsified data into security, safety, and operational systems. This interdependence between cyber and physical domains underscores the challenge of maintaining the confidentiality, integrity, and availability of nuclear data streams in the presence of motivated adversaries.

Another critical insight is that AI systems both benefit from and depend on the data richness of IIoT, yet this reliance creates novel vulnerabilities. Manipulated data streams, adversarial inputs, and data poisoning attacks can compromise the reliability of predictive models, while model inversion, theft, and trojaning introduce strategic risks of espionage, sabotage, and system hijacking.

Unlike traditional SCADA vulnerabilities, these AI-centric threats are subtle, difficult to detect, and potentially catastrophic in their implications. The nuclear sector's near-zero tolerance for error magnifies the consequences of such exploits, demanding assurance strategies that extend far beyond those currently prescribed for industrial environments.

Equally important is the governance and compliance landscape. While frameworks, such as IEC 62443, provide strong foundations for industrial cybersecurity, and ISO/IEC 42001 introduces governance principles for AI, a mature regulatory framework specific to AI-driven IIoT in the nuclear context does not yet exist. This gap means that nuclear operators must proactively adapt existing standards and integrate them with domain-specific requirements, such as those from the IAEA and national regulators. Ethical considerations – including explainability of AI decisions, accountability in case of failures, and bias in training data – further complicate adoption in nuclear applications.

Ultimately, this paper highlights a paradox. On one hand, nuclear facilities do not strictly need IIoT: SCADA and OT systems already provide robust monitoring and control, and existing redundancy practices ensure resilience. On the other hand, the nuclear industry is not insulated from digital transformation: pressures to modernise, improve cost efficiency, and leverage AI for predictive safety analyses will inevitably draw IIoT and AI into the sector. The challenge, therefore, is not whether IIoT and AI should be adopted, but how they can be adopted safely, securely, and ethically – without undermining the fundamental priorities of nuclear safety and reliability.

Going forward, a blended approach may represent the most pragmatic path. This involves combining nuclear-specific guidance (e.g. IAEA's lifecycle management approaches), industrial cybersecurity frameworks (e.g. IEC 62443), and emerging AI governance structures (e.g. ISO/IEC 42001). Such an integrated model would enable nuclear facilities to reap the benefits of advanced data analytics while preserving the sector's safety ethos. Additionally, the human element – ensuring operators remain in the loop, preserving physical inspections, and avoiding over-reliance on automation – will remain central to preventing cascading failures.

In conclusion, while IIoT and AI offer transformative potential for nuclear operations, they also raise fundamental questions about necessity, proportionality, and resilience. The nuclear industry must balance the drive for modernisation with the recognition that introducing new technologies in such a high-stakes environment inevitably carries risks that are unique, amplified, and persistent. By proactively addressing these challenges, the industry can move towards a future where digital innovation complements – rather than compromises – the security and safety foundations of nuclear infrastructure.

VCDNP

Vienna Center for Disarmament and Non-Proliferation

The VCDNP is an international non-governmental organisation that promotes peace and security by conducting research, facilitating dialogue, and building capacity on nuclear non-proliferation and disarmament.

vcdnp.org

@VCDNP

info@vcdnp.org

VCDNP