VCDNP Vienna Center for Disarmament and Non-Proliferation

January 2026

Nuclear Security in a Changing World

Balancing Innovation and Nuclear Security for AI and IoT Technologies

Dr. Sarah Case Lackner
Mara Zarka

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

Authors

Dr. Sarah Case Lackner is a Senior Fellow at the VCDNP. Her work focuses on nuclear security and its interactions with AI and other emerging and disruptive technologies. Among other positions, she was a Senior Nuclear Security Officer at the International Atomic Energy Agency (IAEA), serving as the Scientific Secretary for the Nuclear Security Guidance Committee and the Director General's Advisory Committee on Nuclear Security. She also served as Co-Scientific Secretary of the 2022 Conference of Parties to the A/CPPNM.

Mara Zarka is a Research Associate and Project Manager at the VCDNP, where her research addresses the intersection of emerging and disruptive technologies with nuclear, the security of nuclear and radiological materials against malicious non-State actors, and the non-proliferation regime and nuclear governance. Her work has also included projects on nuclear safeguards and peaceful uses of nuclear technologies, among others.

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

The VCDNP thanks **Global Affairs Canada** for supporting this research project, including the expert workshop and this publication.

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

Internet of Things devices and AI are integrated into both consumer and industrial sectors, offering benefits but also presenting new and expanded risks.

Executive Summary

Data is everywhere, and machines are increasingly able to sense, share, and act on it. A wide range of everyday and industrial devices are equipped with Internet of Things (IoT) capabilities, enabling them to connect to networks and collect and exchange data. Artificial intelligence (AI), in turn, allows computer systems to perform tasks that typically require human intelligence, such as learning, pattern recognition, decision-making, and language processing. Together, these technologies are rapidly spreading across consumer and industrial sectors, driving large-scale data collection and analysis, including in the nuclear sector.

The nuclear industry is increasingly exploring the use of industrial IoT (IIoT) combined with advanced AI systems to enhance safety, security, and operational efficiency in nuclear facilities. When integrated into facilities, these technologies could improve perimeter monitoring and enable predictive maintenance through real-time monitoring of critical equipment and key reactor components. However, greater reliance on IIoT and AI, particularly in high-consequence critical infrastructure such as nuclear facilities, introduces new and expanded security risks, including an increased number of cyber vulnerabilities and novel attack types targeting AI systems.

To examine these challenges and inform policymakers, regulators, and international organisations, the Vienna Center for Disarmament and Non-Proliferation (VCDNP) convened a workshop on 15–16 October 2025, funded by Global Affairs Canada. The workshop brought together 20 technical experts and regulators from across multiple regions and disciplines. Discussions from the workshop informed this report, which assesses the risks and benefits at the intersection of IoT, AI, and nuclear security, and presents conclusions for governments, regulators, industry, and international organisations.

IIoT and AI have the potential to present significant benefits for the nuclear industry. IIoT can provide unprecedented real-time data to support predictive maintenance, operational optimisation, and enhanced monitoring. When combined with AI, these data streams could strengthen situational awareness and decision-making. While secure implementation in the existing fleet of nuclear reactors and other facilities is likely to pose challenges, in new reactor designs, these capabilities can be incorporated securely from the outset.

The widespread integration of IIoT in nuclear facilities will significantly increase the volume of data generated, requiring careful attention to data security and national data sovereignty requirements. At the same time, greater use of IIoT will expand the cyberattack surface, increasing the range of potential cyber security vulnerabilities. AI systems also introduce distinct risks, including novel attack vectors such as data poisoning and adversarial inputs, stemming from how these systems are trained and operate. In addition, AI poses challenges for verification and validation, as its decision-making processes may be opaque or difficult to explain. Long construction timelines in the nuclear sector raise further concerns, as digital systems may be outdated by the time facilities are commissioned, while human-in-the-loop controls, though essential, may be imperfect in rapid-response scenarios. Finally, the integration of AI and IIoT in facilities highlights unresolved issues at the intersection of safety and security. While none of these challenges are insurmountable, they will require sustained attention and careful management.

Five conclusions emerge from this analysis: (1) security resource requirements need to be a central element of IIoT–AI cost–benefit assessments in the nuclear sector; (2) retrofitting existing facilities is likely to present greater technical and economic challenges than integrating IIoT and AI into purpose-designed new builds; (3) nuclear security risks may span operational, safety, security, and IT domains depending on the specific applications of IIoT and AI, making a systems-level approach to nuclear security essential; (4) data governance needs to remain a core priority as automation expands; and (5) understanding human–AI interactions and their impact on security culture will be critical.

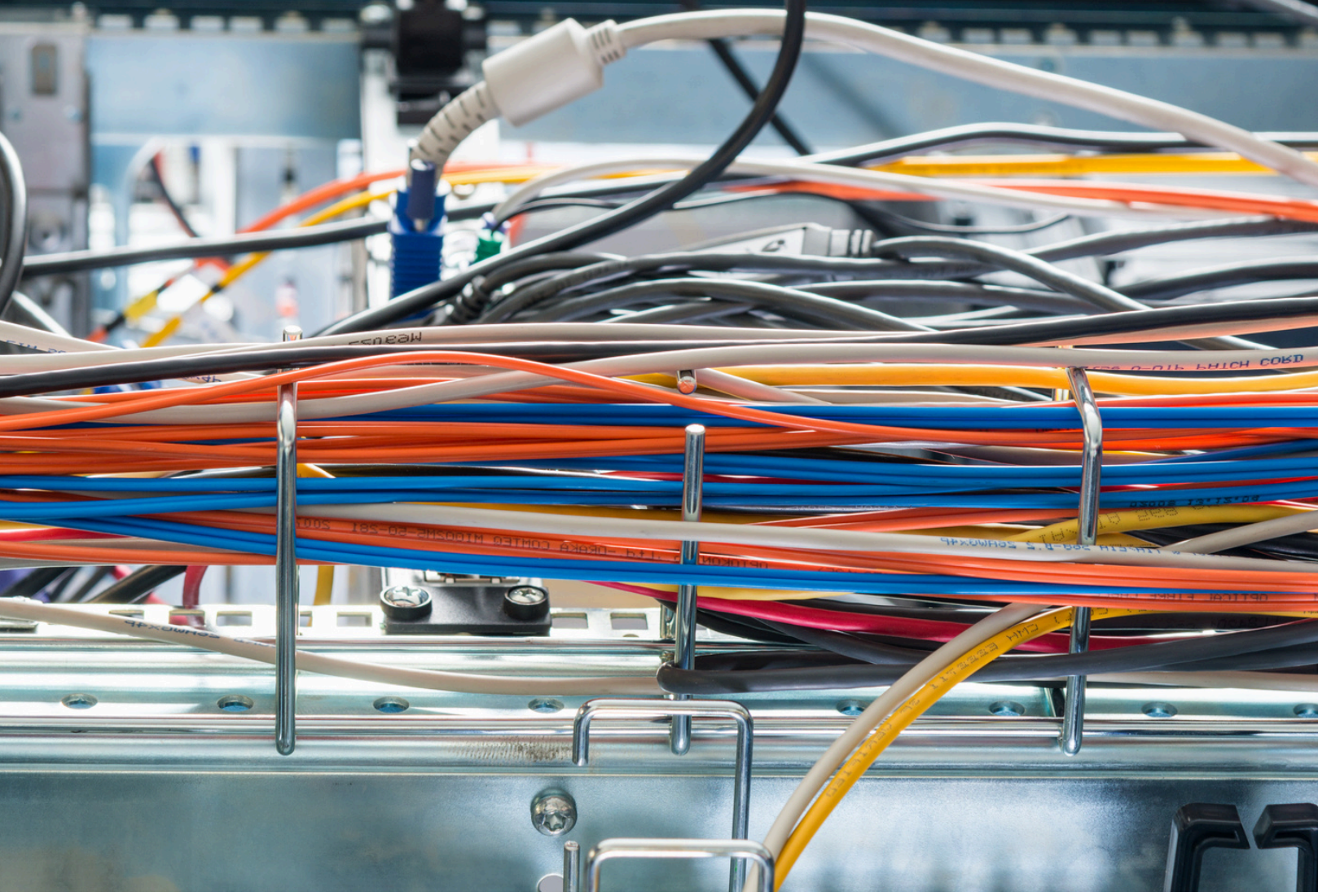
Consumer IoT and publicly available AI introduce a second, distinct category of risk that extends beyond technology intentionally deployed in facilities. IoT capabilities are now embedded in a wide range of everyday devices, sometimes without clear labelling, making inadvertent or malicious introduction into nuclear sites increasingly difficult to prevent. These devices, as well as components inserted through compromised supply chains, can create new entry points for cyber intrusion. At the same time, powerful commercial and open-source AI models give even relatively unsophisticated adversaries enhanced capabilities to analyse open-source and facility data, craft targeted social-engineering attacks, generate malware, and manipulate data streams. Because such risks cannot be eliminated, nuclear security strategies need to emphasise robust controls, improved detection, and strict management of personal and consumer devices.

Four recommendations emerge from the analysis in this report, for the consideration of nuclear security policymakers, regulators, operators, and researchers.

- **In highly digitalised nuclear facilities using IIoT and AI, nuclear security, especially cyber security, should prioritise reliability and resilience over the unrealistic goal of preventing every attack.** Reliability is an aspect of prevention that seeks to prevent the consequences rather than the threat, by eliminating opportunities for digital systems to affect fundamental safety functions. Resilience addresses ensuring that facilities can return to safe, stable operation quickly after an incident, a key aspect of response.
- **Cost-benefit assessments for IIoT and AI integration should account for physical and cyber security measures needed to maintain robust nuclear security when these technologies are used.** This calculation is likely to be different for new designs and for existing facilities as well as older designs being prepared as new builds.

- **The nuclear sector should proactively learn from other critical infrastructure sectors that are advancing more rapidly in digitisation and in the use of IIoT and AI.** Policymakers should seek opportunities to establish mechanisms for systematic knowledge-sharing with these sectors, drawing on their experience to strengthen nuclear security and avoid repeating avoidable mistakes.
- **Up-to-date, practical guidance for operators and regulators on maintaining nuclear security in a rapidly changing environment should be continuously developed and shared by international and other relevant organisations, including NGOs and industry groups.** New security challenges arising from AI and its links to IoT are evolving faster than current international and national advice and information can address.

Preparing now – by embedding cyber and physical security from design, investing in workforce capabilities, and fostering international collaboration – will allow decision makers to harness IIoT and AI benefits while managing the realistic, evolving risks these technologies are likely to bring.



The digital transformation is changing how our lives are managed and how industry operates.

Introduction

New technologies are rapidly changing the world as we know it. The digital transformation, which has been ongoing since the 1950s and accelerated around the turn of the last century, is now giving way to another sweeping set of changes in how our everyday lives are managed and how industry operates. One key element of this latest revolution is increased automation of a broad range of tasks via artificial intelligence (AI) and its interactions with Internet of Things (IoT) devices.

AI and IoT are transforming both consumer and industrial sectors. On the consumer side, IoT devices and AI can simplify and automate the everyday operation of homes and communities. IoT devices provide new sources of data for AI to process and even act on, such as sensing fires, improving electrical efficiency, or automatically ordering more milk when none is left in the refrigerator. On the industrial side, usually referred to as IIoT (industrial internet of things), both IoT devices and AI are integrated into industrial processes to improve efficiency, productivity, and save costs.

In the nuclear sector the vast amount of digitised data that could be generated by IIoT devices could provide opportunities for AI to enhance safety, security, and efficiency in nuclear facilities, for example, by improving perimeter monitoring for security or by enabling predictive maintenance based on real-time monitoring of critical equipment, such as turbines, pumps, and cooling systems, as well as key reactor components.[1]

1 Donald Dudenhoeffer, “Internet of Things and the Impact on Nuclear Facilities”, VCDNP and AIT, Jan 2026, p. 14. Available at: https://vcdnp.org/wp-content/uploads/2026/01/IoT.pdf.

However, an increase in the use of these technologies in nuclear facilities will also be accompanied by novel and expanded security risks that will need to be managed and mitigated. The introduction of IIoT devices will increase the number of potential cyberattack pathways, and AI itself will introduce novel attack types. Further, the increasing use of AI and IoT on the consumer side may also provide adversaries with additional opportunities and even new tools to attack nuclear facilities.

With this in mind, the Vienna Center for Disarmament and Non-Proliferation (VCDNP) convened a workshop on 15 and 16 October 2025, entitled "Nuclear Security in a Changing World: Exploring Evolving Nuclear Security Risks Associated with the Internet of Things and AI." The workshop, which focused on how to manage this shifting landscape for national policymakers, regulators, and international organisations, was funded by Global Affairs Canada and convened 20 technical experts in IoT, AI, cyber security, nuclear engineering, and nuclear security. Participants brought a wide range of international perspectives, coming from the nuclear industry, research and academia, international organisations, and nuclear laboratories across Africa, Europe, North America, South America, the Asia-Pacific, and the Middle East. The workshop also included a discussion session providing technical experts with an opportunity to review their initial conclusions with national regulators from Europe, Africa, North America, and South America.

The two days of discussions informed the development of this report, which highlights risks and benefits at the intersection of IoT, AI, and nuclear security, and offers conclusions for national governments, national regulatory bodies, industry, and international organisations to consider.

Understanding IoT and AI technologies, their capabilities, and limitations, is necessary to implement appropriate security measures for their use in nuclear facilities. Photo: The Doel nuclear power plant near Antwerp, Belgium.

Impacts of IoT and AI on Nuclear Security

Efforts to inform policymakers and regulators about the nuclear security implications of emerging technologies are often hindered by the complexity of the technologies themselves. Effectively assessing the benefits, security risks, and necessary security measures for integrating IoT and AI systems requires a foundational understanding of these technologies and their practical capabilities and limitations.

To address this need, the following section provides a brief introduction to IoT and AI, and explains their potential uses in nuclear facilities, with links to reports that provide additional background where beneficial.

Internet of Things (IoT) and Industrial Internet of Things (IIoT)

The term Internet of Things was first coined in 1999 by Kevin Ashton to describe "a system where the Internet is connected to the physical world via ubiquitous sensors."[2] Today, the Internet of Things (IoT) refers more broadly to network-enabled physical devices that can collect and exchange data. Although the term persists, modern IoT devices are not always connected to, or intended to connect to, the broader internet. Instead, they rely on a network (e.g. cellular, Bluetooth, or radio frequency identification) to communicate, share data, and perform tasks. IoT devices are now used in a wide range of applications, from smart home appliances to industrial sensors such as vibration and temperature monitors.

2 Avnet Silica, "Interview with Kevin Ashton – inventor of IoT: Is driven by the users", Avnet Siliva, 11 February 2018. Available at: https://my.avnet.com/silica/resources/article/interview-with-iot-inventor-kevin-ashton-iot-is-driven-by-the-users/.

The choice of network architecture often influences the efficiency and reliability of data transmission.[3]

In 2012, General Electric introduced the term Industrial Internet of Things (IIoT) to describe the application of IoT technologies in industrial settings such as manufacturing, transportation, and energy.[4] In this report, IIoT refers specifically to the industrial applications of IoT, while IoT denotes either all IoT devices or, more narrowly, consumer devices.[5]

IIoT architecture is based on four key layers that manage the information collected by these devices and analyse and process the data they produce, as illustrated in Figure 1 below.[6] Figure 1 depicts a conceptual overview of the IIoT architecture with the four layers (perception, network, processing, and application) listed on the left hand side, and two key data management strategies indicated under the processing layer (edge and cloud computing).

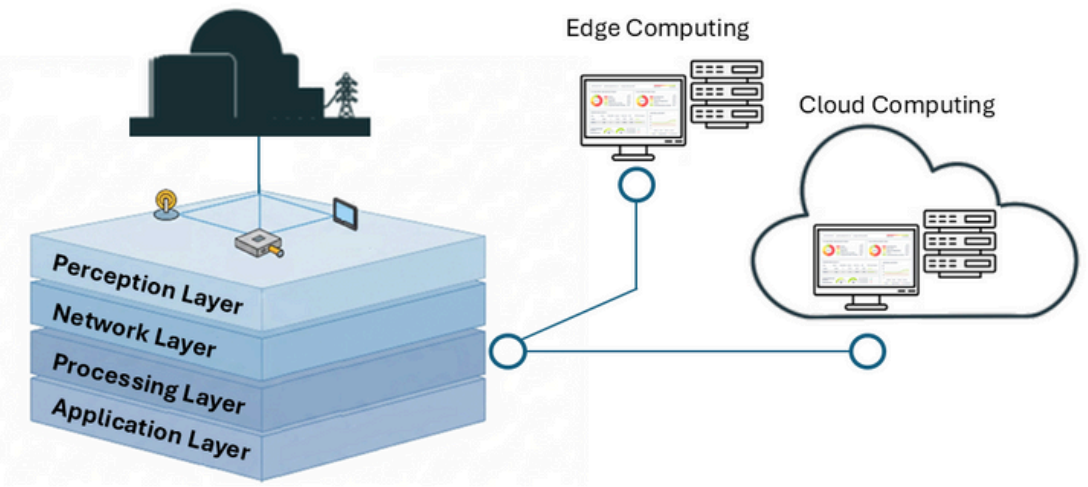


Figure 1. IIoT Framework Overview[7]

These layers, the perception, network, data processing, and applications layers, operate as follows.

- The **Perception Layer**, also referred to as the sensing layer, collects raw data from the physical environment via sensors, actuators, radio frequency identification tags, and other embedded devices. This layer enables real-time data collection, for example, of temperatures or radiation levels across various parts of a nuclear power plant.
- The **Network Layer**, also referred to as the connectivity or communication layer, allows for digital data to move securely from one device, system, or application to the next. This layer requires infrastructure sufficient to support data extraction from the perception layer and its transport to the processing layer, whether via cabled connections, wireless, or secure private 5G networks.[8]

3 Device Authority, "Understanding IoT Networks: A Beginner's Guide", accessed in November 2025. Available at: https://deviceauthority.com/understanding-iot-networks-a-beginners-guide/.

4 Cisco, "What is industrial (IIoT)?" Cisco, accessed in November 2025. Available at: https://www.cisco.com/site/us/en/learn/topics/industrial-iot/what-is-industrial-iot.html.

5 For more detailed information on IoT and IIoT, see Lobna Ben Khelifa, "Cyber Security in IoT/IIoT and AI Integration", VCDNP, Jan 2026, for its specific application to nuclear facilities, see Donald Dudenhoeffer, "Internet of Things and the Impact on Nuclear Facilities", VCDNP and AIT, Jan 2026, and for cyber security implications in the nuclear sector, see Khalil El-Khatib and Pooria Madani, "Data Security Challenges in the Integration of IIoT and AI in the Nuclear Industry", VCDNP, Jan 2026.

6 Device Authority, "Unpacking IoT Architecture: Layers and Components Explained", accessed in Nov 2025. Available at: https://deviceauthority.com/unpacking-iot-architecture-layers-and-components-explained/.

7 Donald Dudenhoeffer, "Internet of Things and the Impact on Nuclear Facilities", VCDNP and AIT, Jan 2026, p. 3. Available at: https://vcdnp.org/wp-content/uploads/2026/01/IoT.pdf.

8 More detail can be found on the specific challenges of retrofitting nuclear power plants to include networking infrastructure to support IIoT in Donald Dudenhoeffer, "Internet of Things and the Impact on Nuclear Facilities", VCDNP and AIT, Jan 2026. Available at: https://vcdnp.org/wp-content/uploads/2026/01/IoT.pdf.

- The **Data Processing Layer**, also known as the computing layer, processes and analyses data received from the network layer to generate insights and support decision-making. This layer may use AI to manage large data volumes and distil them into more meaningful elements, employing edge, cloud, or hybrid computing for these functions.[9]
- The **Application Layer**, also known as the user interface layer, provides interfaces for end-users to interact with the IIoT architecture. For example, data from IIoT devices or AI-generated recommendations might be presented to operators through a centralised dashboard on a computer or mobile device.

Security can be considered as an additional cross-cutting layer of the IIoT framework, applicable to all four layers above:

- The **Security Layer** ensures that "all devices, connections, and data stored are secure."[10] This layer includes security measures such as encryption for data transmission, user verification, and access controls. These are supplementary controls applied to manage residual risks that remain when inherent risks cannot be fully addressed during the design and engineering phase.

The data processing layer is critical when considering applications that integrate AI systems with IIoT. Given AI's substantial computing demands and the stringent data security and data sovereignty requirements in the nuclear sector, careful consideration of where and how IIoT data is processed is essential. There are several possible options that can be combined to create hybrid approaches, depending on the application and other requirements:[11]

- **Edge Computing**, in which data is processed and analysed close to the source of data generation. In this case, data is managed and stored locally on an "edge device", which can operate as a standalone device in the local network, without a need for internet connection. It allows for on-premises analysis, reduces latency,[12] and minimises storage demands, since data is processed on the edge device and does not need to be transferred to a cloud storage or data centre for further processing. This approach can be helpful for real-time data analysis, enabling near-instantaneous processing and sending only relevant data to central servers for broader analysis.
- **Cloud Computing**, which relies on centralised data centres, accessed via the internet, to store and process large volumes of data. In its purest form, IIoT devices send raw data to be processed by remote servers, where a broad spectrum of analytics can be performed, although the data could also be pre-processed by edge devices. Cloud computing offers scalability by providing a flexible and cost-effective infrastructure as well as longer term storage and analysis. It may be needed for some AI applications due to high needs for computing power. Due to higher latency, cloud computing is better suited for non-time sensitive data processing.
- **On-premises or corporate centralised computing**, which refers to computing infrastructure physically located within an organisation's facilities and operated under its direct control. In this model, data is processed, stored, and managed on-site rather than being transmitted to external cloud services. This approach allows organisations to maintain greater oversight of system performance, data security, and compliance with internal policies or regulatory requirements, but typically requires substantial investment in hardware, maintenance, and technical expertise.

9 For an explanation of edge, cloud, and hybrid computing see Lobna Ben Khelifa, "Cyber Security in IoT/IIoT and AI Integration", VCDNP, Jan 2026, pp. 7-8, and Donald Dudenhoeffer, "Internet of Things and the Impact on Nuclear Facilities" VCDNP and AIT, Jan 2026, p. 7.

10 Device Authority, "Unpacking IoT Architecture: Layers and Components Explained", accessed in Nov 2025. Available at: https://deviceauthority.com/unpacking-iot-architecture-layers-and-components-explained/.

11 Tiffany Yeung, "What's the Difference Between Edge Computing and Cloud Computing?" NVIDIA, 5 Jan 2022. Available at: https://blogs.nvidia.com/blog/difference-between-cloud-and-edge-computing/.

12 Latency refers to the delay in time for data to be transferred.

A **combined approach** is also possible, allowing organisations to deploy real-time data processing on the edge while benefiting from long-term data analytics and storage in the cloud or at centralised corporate data centres.

When implementing an IIoT framework in a critical industry such as the nuclear sector, it is important to consider the implications of increased integration between Information Technology (IT) and Operational Technology (OT) systems, as noted by Ben Khelifa (2026).[13] This convergence may introduce new risks, depending on the application, including:[14]

- **Expanded Attack Surface**: Compromises on the IT network could provide pathways into critical OT networks.
- **Incompatible Security Postures**: Many legacy OT systems were designed for reliability and safety rather than security and may be incompatible with currently standard IT security tools.
- **Catastrophic Consequences**: Successful attacks could result in physical damage, environmental disasters, and prolonged production downtime.

The magnitude of these risks depends on the specific application being considered and, in many cases, can be mitigated through a strong defensive computer security architecture.

From a business perspective, implementing an IIoT framework in a nuclear facility will require a cost-benefit analysis, as discussed in the next section of this report. Further, it will also necessitate a range of agreements and contracts for procurement of IIoT devices, compliance with regulatory requirements and national laws, and development of policies, procedures, and structures for implementing IIoT solutions and their use.

Artificial Intelligence Models and Systems

The term AI models and systems encompasses a range of tools designed to emulate aspects of human cognition, enabling tasks such as pattern recognition in large datasets, image and speech processing, decision-making, and text or image generation.[15] AI models are the trained algorithms that use machine learning[16] to generate predictions or outputs from data, while AI systems are the complete applications that use these models to perform specific tasks in real-world settings. Recent advances in machine learning and supporting technologies have significantly accelerated the development and use of these models and systems. The term "AI" will be used throughout this report to refer to "AI models and systems" where specificity on whether a model or system is meant is not needed.

AI can be broadly categorised as predictive, generative, or agentic. Predictive AI uses statistical and machine learning methods to analyse data and support tasks such as forecasting, anomaly detection, and classification. Generative AI creates new or derived content by identifying patterns and relationships in their training data: current systems can generate text, images, code, audio, and other modalities and can synthesise information across diverse data sources.[17] Agentic AI systems, still in early development, use various techniques to pursue tasks and goals with limited human oversight. These systems can break objectives into steps, use external software tools, adapt to new information, and, in some architectures, maintain memory of past actions.

13 Lobna Ben Khelifa, "Cyber Security in IoT/IIoT and AI Integration", VCDNP, Jan 2026, p.13. Available at: https://vcdnp.org/wp-content/uploads/2026/01/Cyber Security.pdf.

14 Ibid.

15 More detailed discussion on AI models and systems aimed at policymakers can be found in Sarah Case Lackner and Zaheed Kara, "Artificial Intelligence Models and Systems", Emerging Tech Brief No. 1, VCDNP, 2025, and in Sarah Case Lackner and Mara Zarka, "Nuclear Security and the Nuclear Supply Chain in the Age of Artificial Intelligence", VCDNP, April 2025, pp. 4-6.

16 Machine learning is a method enabling software models to identify patterns in data without being explicitly programmed to do so.

17 A more detailed discussion of generative AI is available in Natasha E. Bajema, "Generative AI and WMD Nonproliferation: A Practical Primer for Policymakers and Diplomats", CNS Occasional Paper, No. 63, Dec 2024. Available at: https://nonproliferation.org/wp-content/uploads/2024/12/generative_ai_and_wmd_nonproliferation_12042024.pdf.

AI can also be categorised as either purpose-specific or general-purpose. A purpose-specific system may be trained to identify anomalies in a particular type of input data, drawing on patterns learned during its training. While most of the examples of AI addressed in this report are purpose-specific, general-purpose models, such as commercial or open-source large language models (LLMs), are also relevant to nuclear security, particularly because they can enhance an adversary's ability to process information or generate computer code.[18]

When AI is used to process data from IIoT systems, it is typically implemented within the data processing layer of the IIoT framework described above. These systems analyse large volumes of IIoT data to identify anomalies or operational insights that support human decision-making, and in some cases may also automate certain decisions or responses, such as in cyber security applications.

AI requires substantial data flows and computing resources to effectively operate, and some applications may exceed the capacity available on-site. As noted in the previous section, dedicated corporate data centres can meet some of these needs, but many industries routinely rely on cloud computing: uploading data for remote processing. However, as discussed later in this report, cloud-based solutions may raise data security and data sovereignty concerns in the nuclear sector.[19] In some cases, these concerns can be mitigated through edge computing, which enables local pre-processing and reduces both the volume and sensitivity of data sent to external providers.

AI, IoT, and Nuclear Security

When integrating AI or IoT devices into nuclear facilities to improve operations, support decision-making systems, or strengthen security, nuclear security considerations need to be taken into account from the outset. These technologies have the potential to introduce new risks, such as expanded and novel cyberattack pathways and the potential manipulation of data produced by AI systems intended to support operator decisions. At the same time, the widespread availability of consumer IoT devices and powerful, commercially available and open-source AI models provides adversaries with new tools.

In the remainder of this report, the security implications of IoT and AI will be examined in greater depth, beginning with the potential impacts of intentionally integrating these technologies into nuclear facilities. The nuclear security implications of consumer IoT and publicly available AI models will be considered separately.

18 For a more detailed discussion on adversary capabilities using general-purpose systems, see Sarah Case Lackner and Zaheed Kara, "Artificial Intelligence and Nuclear Security Governance: Addressing the Risks of Frontier AI", VCDNP, Dec 2025. Available at: https://vcdnp.org/wp-content/uploads/2025/12/VCDNP_AI-and-Nuclear-Security-Governance_web.pdf.

19 Details on applications of AI for nuclear facilities can be found in Donald Dudenhoeffer, "Past, Present, and Future Applications of AI in the Nuclear Sector", VCDNP and AIT, Apr 2025. Available at: https://vcdnp.org/wp-content/uploads/2025/04/VCDNP-AIT_Past-Present-and-Future-Applications-of-AI-in-the-Nuclear-Sector_web.pdf.

Ensuring strong physical and cybersecurity is essential when considering integrating technologies, like IIoT and AI, in nuclear facilities.

Nuclear Security Implications of IIoT and AI Integrated into Nuclear Facilities

The integration of IIoT and AI technologies into nuclear facilities can offer substantial benefits, such as improved predictive maintenance, optimised operations, and enhanced monitoring capabilities for nuclear security. At the same time, these technologies introduce new and amplified nuclear security risks that need to be carefully managed. The following two sections examine these implications by: (1) outlining the opportunities and challenges associated with technology adoption in the nuclear sector; (2) identifying key considerations for balancing the security risks and benefits of IIoT and AI integration; and (3) presenting conclusions to guide stakeholders evaluating their use.

Technology Adoption in the Nuclear Sector

Technology adoption in the nuclear sector is generally slower than in many other industries, including other critical infrastructure sectors. This is due in part to factors that are particularly pronounced or unique in the nuclear domain, such as the age of many facilities, long construction timelines, the high-consequence nature of safety or security incidents, and stringent regulatory requirements that create multiple hurdles for integrating new technologies.

Most nuclear power plants in operation today were built in the 1970s and 1980s, with a global average age of 32 years as of 2025.[20] As these facilities age, electromechanical systems need to be replaced to maintain safety and operational performance, which can create opportunities to introduce new technologies. However, upgrading older plants can be challenging, as they were not designed for digitisation or for modern systems such as IIoT or AI, making integration significantly more complex.

These challenges lead some to question the value of incorporating digital technologies, let alone IIoT or AI, into existing nuclear facilities. While such facilities may not require IIoT or AI, they may still adopt them if the benefits are sufficiently compelling. Moreover, even facilities that wish to avoid these technologies may have limited choice: when ageing components fail and replacement parts often include built-in networking (IIoT) capabilities that cannot always be disabled and may not be clearly identified by manufacturers or installers. By contrast, new designs, such as Small Modular Reactors and other advanced reactors have the opportunity to anticipate and plan for IIoT and AI integration, as well as associated security considerations, including cyber security considerations, in the design process. In all cases, decisions to adopt IIoT or AI technologies should be guided by a risk–benefit analysis, accounting for the kinds of factors outlined in this section.

Technology integration in the nuclear sector is further complicated by the long timelines associated with building new facilities. Nuclear reactors generally take longer to construct than most other power generation options, aside from some large hydropower projects, and longer than many major infrastructure projects. A study of reactors built between 1976 and 2009 found an average construction duration of 92 months (7.7 years), measured from groundbreaking to initial operation.[21] This figure excludes the additional years required for design licensing, environmental reviews, and siting permits, all of which precede construction.

Because of the long interval between reactor design and completion of construction, new nuclear builds often rely on designs that are already decades old. Digital technologies, however, evolve far more rapidly, meaning that systems approved early in the design process may be outdated by the time a plant enters operation. Updating technologies during design or construction is possible, but typically triggers additional regulatory review, further extending project timelines. The Barakah-4 reactor recently completed in the United Arab Emirates illustrates this challenge: the APR1400 design began development in 1992 and was approved for use in South Korea in 2002.[22,23] An application submitted to the U.S. Nuclear Regulatory Commission for a Standard Design Certification in 2013 was not approved until 2018.[24,25,26] Construction of Barakah-4 began in 2015, and the unit entered commercial operation in 2024, over 30 years after initial design work began. This extended timeline is not unusual in the nuclear sector.

A further factor slowing the integration of new technologies is the widely recognised potential severity of safety or security incidents at nuclear facilities. At fuel-cycle facilities or sites storing nuclear material, theft could enable the construction of a crude nuclear device. At other facilities, including nuclear power plants, an accident or act of sabotage that compromises safety systems could result in a significant radiation release with long-lasting environmental and human consequences.

20 Peter Hannam, “The Coalition says its nuclear plants will run for 100 years. What does the international experience tell us?” The Guardian, 24 Jun 2024. Available on the World Nuclear Industry Status Report website, posted 27 Jun 2024: https://www.worldnuclearreport.org/The-Coalition-says-its-nuclear-plants-will-run-for-100-years-What-does-the.

21 Pedro Carajilescov and Joao M.L. Moreira, “Construction time of PWRs”, International Nuclear Atlantic Conference – INAC 2011, Oct 2011, ISBN 978-85-99141-04-05. Available at: https://inis.iaea.org/records/bgsm3-a1y30.

22 The design of Barakah-4 is an Advanced Power Reactor 1400 (APR1400), designed by Korea Electric Power Corporation (KEPCO) and Korea Hydro and Nuclear Power Co., starting in1992. The design was approved for use in South Korea in 2002. Barakah Units 1, 2 and 3, all APR 1400 designs, started commercial operation in 2021, 2022 and 2023, respectively.

23 Han Ok Kang, Byung Jin Lee, and Sang Gyu Lim, “Light water SMR development status in Korea”, Nuclear Engineering and Design, Vol. 419, 1 Apr 2024. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0029549324000682.

24 U.S. Nuclear Regulatory Commission, “Issue Design Certification – Advanced Power Reactor 1400 (APR1400)”, accessed in Nov 2025. Available at: https://www.nrc.gov/reactors/new-reactors/large-lwr/design-cert/apr1400.,

25 World Nuclear News, “Korean reactor design certified for use in USA”, 27 Aug 2019. Available at: https://www.world-nuclear-news.org/articles/korean-reactor-design-certified-for-use-in-usa.

26 U.S. Nuclear Regulatory Commission, “Standard Design Approval for Advanced Power Reactor 1400”, 28 Sep 2018. Available at: https://www.nrc.gov/docs/ml1826/ml18261a187.pdf.

The nuclear industry prioritises safety, informed by past events such as Chernobyl (1986) and Fukushima (2011), which demonstrated that a single accident could slow global nuclear development for decades. Although no severe nuclear security incident has occurred, it is widely recognised that its consequences could be similarly far-reaching. As a result, the sector generally favours cautious, incremental modernisation over rapid innovation, shaping its approach to adopting digital technologies, including IIoT and AI.

Given the potentially catastrophic consequences of a failure, national regulatory requirements for nuclear facilities are necessarily stringent. Regulators typically mandate extensive documentation for design licensing, environmental assessments, and construction and operating permits, all of which incorporate safety and security considerations. Meeting these requirements is a complex and highly technical process, as demonstrated by the International Atomic Energy Agency's (IAEA) publication of more than 130 Safety Standards[27] and over 40 Nuclear Security Series[28] guidance publications to support states in ensuring safe and secure nuclear operations.

Thus, new technologies, regardless of their benefits, can only be adopted if they do not compromise safety and security. In many cases, additional security measures will be required, and these need to be weighed against the expected benefits of the technologies—a topic addressed in the next section.

Balancing Security Risks and Benefits of IIoT and AI Integration

Decisions to integrate IIoT and AI technologies into nuclear facilities require operators to weigh the expected benefits against the associated costs, including for security measures. Regulators need to make similar assessments when licensing designs or approving specific technologies. The following sections outline the potential benefits of IIoT and AI for both new and existing facilities, followed by the key risks and costs to be considered when evaluating their adoption.

Benefits of IIoT and AI in Nuclear Facilities

Effective integration of IIoT and AI in nuclear facilities can improve operational efficiency by providing more comprehensive and timely information about facility conditions, whether normal or anomalous. IIoT devices generate large volumes of real-time plant data, which AI systems can analyse and translate into actionable insights to support decision-making in operations, safety, and security.

Dudenhoeffer (2026) identifies several potential applications of IIoT and AI in nuclear power plants, including condition monitoring and predictive maintenance, enhanced safety and emergency management, improved operational efficiency, cyber security integration, digital twins, inventory and supply chain management, and remote monitoring and control.[29]

Security systems, both physical and cyber, can also significantly benefit from IIoT and AI technologies. Current applications include anomaly detection, intrusion detection, and automated alert assessment. By rapidly analysing large data sets across multiple systems, IIoT and AI could also identify patterns and anomalies that span otherwise unrelated systems, revealing connections that might not be apparent through traditional analysis.

AI and IIoT are also valuable for enhancing nuclear security, via current and emerging applications such as video analytics, access control and identity verification, tamper detection, cyber anomaly detection, intrusion detection, and alarm assessment and management. All these functions rely on processing large volumes of data to identify anomalous patterns or behaviours.

27 The IAEA Safety Standards are published under the IAEA Safety Standards Series, available at: https://www.iaea.org/resources/safety-standards.

28 The IAEA Nuclear Security Series (NSS) provides consensus guidance on nuclear security for states, available at: https://www.iaea.org/resources/nuclear-security-series.

29 Details on these applications can be found in Donald Dudenhoeffer, "Internet of Things and the Impact on Nuclear Facilities", VCDNP and AIT, Jan 2026. Available at: https://vcdnp.org/wp-content/uploads/2026/01/IoT.pdf.

Nuclear Security Risks of IIoT and AI in Nuclear Facilities and Potential Mitigations

When evaluating whether to integrate technologies such as IIoT and AI into a nuclear facility, the expected benefits need to outweigh the associated costs, including security-related costs. If security risks are not addressed early, the later addition of necessary protections, or the consequences of a security incident, may outweigh any gains. It is therefore essential to assess the security risks of each application, determine the measures required to reduce those risks to an acceptable level, and account for the costs of implementing them. The following subsections outline key nuclear security risk areas for consideration and identify potential mitigation options, either currently available or under active development.

Data Protection and Data Sovereignty

Digitised data is fundamental to the operation of both IIoT and AI. In nuclear facilities, IIoT devices may generate a wide array of information about plant operations, which could be used directly by operators or transmitted to AI systems for further processing and analysis. This processed information can enhance situational awareness and support more informed decision-making. To enable these benefits, the confidentiality, integrity, and availability of the data need to be ensured throughout its lifecycle. In addition, depending on national legislation and regulatory frameworks, facilities may need to comply with specific data sovereignty requirements governing how and where sensitive data is stored and processed.

- **Data Confidentiality:** Nuclear facilities handle multiple categories of sensitive information, including classified data, nuclear-sensitive and safeguards information, export-controlled data, business-sensitive material, privacy data, and other restricted information.[30] IIoT–AI systems may generate or rely on data that falls into one or more of these categories, making robust confidentiality protections essential. The specific measures required will depend on the facility, the intended application, and the sensitivity of the data, and should be applied using a graded approach. Common measures include encryption, strong access controls, and the use of controlled communication between security zones.

- **Data Integrity:** Ensuring the integrity of data generated by IIoT devices and used by AI systems is equally critical. Data need to remain accurate, complete, and consistent throughout its lifecycle, as the reliability of both operator decisions and AI-generated outputs depends on its integrity. This includes maintaining the integrity of training data used to develop AI models as well as the operational data provided to them in real time. Any manipulation, whether accidental or malicious, can lead AI systems to produce incorrect conclusions, potentially affecting plant operations or safety.

- **Data Availability:** Ensuring that data is accessible when needed is also essential, as AI systems rely on timely inputs to generate accurate assessments. Disruptions to data availability, whether caused by technical failures or deliberate attacks, can prevent AI systems from receiving critical information. For example, an adversary could block or delay IIoT data from feeding into an AI tool used to inform operators about plant conditions, leading to incorrect conclusions that could affect operational decisions.

- **Data Sovereignty:** Data sovereignty requirements in many countries mandate that sensitive information be stored and processed within national borders. These rules can pose challenges for AI solutions that rely on cloud-based processing or external data storage. As a result, data sovereignty considerations need to be addressed early when selecting AI systems for nuclear facilities, including determining whether their intended functions can be supported without transferring sensitive data outside the country.

30 IAEA, "Security of Nuclear Information", IAEA Nuclear Security Series, No.23-G, 2015. Available at: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1677web-32045715.pdf.

Data Quality and Quantity for AI Model Training

In addition to data protection and data sovereignty considerations, it is crucial to assess whether sufficient, high-quality data is available to train an AI model and to verify its provenance. At present, there is a well-recognised shortage of real-time data from operating nuclear power plants, and obtaining adequate volumes of high-quality operational data is challenging.[31] As a result, many AI models intended for nuclear applications rely heavily on synthetic data that replicates the patterns of real datasets.[32] However, ensuring that synthetic data captures the full range of possible operating conditions, including abnormal states that could result from an adversary's actions, is technically challenging. This limitation increases the risk that AI may fail to recognise certain abnormal or maliciously induced conditions and should be factored into evaluations of potential AI applications.

AI Model Security

The security of AI models themselves also needs to be ensured. AI systems possess unique vulnerabilities because of how they are trained and operate; attackers may target training data, model weights, inference endpoints, or the underlying algorithms. AI model security aims to ensure that models function as intended, resist manipulation, and comply with privacy requirements throughout their lifecycle.

If training data is corrupted (or "poisoned") the model may produce unexpected or unsafe outputs. Research by Anthropic and the Alan Turing Institute indicates that even a small, constant amount of poisoned data can meaningfully influence model behaviour.[33] Adversarial attacks pose an additional risk: by supplying subtly altered inputs, adversaries can cause AI systems to misclassify information or generate incorrect recommendations without the manipulation being apparent to operators. Other risks relevant to particular applications include model inversion, in which adversaries infer sensitive model details from outputs (applicable to many AI models and systems), and prompt injection, which can redirect or compromise generative AI behaviour. Addressing these risks requires specialised AI security strategies, some of which may be adapted from sectors that have adopted AI more rapidly.

Validation and Verification of AI Systems

Reliable methods for validating and verifying AI systems for use in nuclear facilities are still evolving.[34,35] Although research into AI models with explainable reasoning is advancing, it remains challenging to determine precisely how machine learning systems reach their conclusions.[36,37] Because these models identify patterns across vast training datasets without explicit human-defined rules, their reasoning may differ from human expectations.

Given this challenge—and the need for high confidence in AI-generated assessments—operators need to ensure the reliability of both the training data and the model itself. They also need to verify that the system produces expected outputs across likely operating conditions and, to the extent possible, confirm that neither the data nor the model has been compromised, as discussed in the previous section.

31 Anna Hall and Vivek Agarwal, "Barriers to adopting artificial intelligence and machine learning technologies in nuclear power", Progress in Nuclear Energy, Vol. 175, Oct 2024. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0149197024002452.

32 Z. Ma, et al., "Exploring Advanced Computational Tools and Techniques with Artificial Intelligence and Machine Learning in Operating Nuclear Plants", U.S. Nuclear Regulatory Commission, NUREG/CR-7294, INL/EXT-21-61117, Feb 2022. Available at: https://www.nrc.gov/docs/ML2204/ML22042A662.pdf.

33 Alexandra Souly, et al., "Poisoning Attacks on LLMs Require a Near-constant Number of Poison Samples", arXiv preprint arXiv: 2510.07192v1, 8 Oct 2025. Available at: https://arxiv.org/pdf/2510.07192.

34 Sarah Case Lackner and Mara Zarka, "Nuclear Security and the Nuclear Supply Chain in the Age of Artificial Intelligence", VCDNP, Apr 2025. Available at: https://vcdnp.org/wp-content/uploads/2025/04/VCDNP_AI-and-Security-of-the-Nuclear-Supply-Chain_web.pdf.

35 National Institute of Standards and Technology, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)", U.S. Department of Commerce, NIST AI 100-1, Jan 2023. Available at: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

36 Azza Mohamed, Khaled Abdelqader, and Khaled Shaalan, "Explainable Artificial Intelligence: A systematic Review of Progress and Challenges", Intelligent Systems with Applications, Vol. 28, Dec 2025. Available at: https://www.sciencedirect.com/science/article/pii/S2667305325001218.

37 Bowen Long, et al., "Explainable AI the Latest Advancements and New Trends", arXiv preprint arXiv: 2505.07005, 11 May 2025. Available at: https://arxiv.org/abs/2505.07005.

While active research is addressing these issues, further progress is needed before comprehensive validation and verification approaches are available.[38]

Increased Cyberattack Surface

As nuclear facilities evolve from hundreds to thousands (or even tens of thousands) of interconnected devices, IIoT will enable unprecedented data collection and analysis, but will also increase the cyberattack surface and the potential range of cyber vulnerabilities. This challenge is not unique to the nuclear sector; energy, finance, manufacturing, transportation, and other industries are encountering similar risks as IIoT adoption grows. Although it is unrealistic to eliminate all vulnerabilities in such complex, highly networked environments, robust cyber security measures applied across all integrated devices can significantly reduce the likelihood of a successful attack.

As discussed further later in this report, these measures need to address not only IIoT systems used for operations, safety, or security but also consumer-level IoT devices that may be intentionally or inadvertently brought into or near the facility. Common examples include smartphones, smart displays in conference rooms, and connected appliances in break areas, all of which can introduce additional cyber security risks if unmanaged.

Human Factors

The integration of IIoT and AI into nuclear facilities involves not only their interaction with plant infrastructure but also with personnel. Most discussions on AI adoption in the nuclear sector emphasise the need to maintain a "human-in-the-loop."[39] This is particularly important for any actions affecting safety. Staff serving in this role need to be trained to interpret AI outputs, understand the strengths and limitations of AI systems, and critically assess recommendations rather than accepting them at face value. Without this expertise, operators may fail to recognise malicious data manipulation or other adversarial attacks, even when warning signs are present. However, even with adequate training, a human-in-the-loop may not be an adequate control for decisions that need to be made rapidly or in real time.

Effective human–AI interaction also requires familiarity with the psychology of how operators engage with automated systems, an area of research that is active but still emerging, including within the nuclear field.[40] In addition, all staff interacting with AI systems, whether directly involved in nuclear security or not, should be grounded in robust nuclear security culture to ensure vigilance. The IAEA's Nuclear Security Series provides widely respected guidance for strengthening security culture, although it does not yet specifically address AI-human interaction.[41]

Vendors

Nuclear facilities typically take multiple years to construct, which is far longer than the lifecycles of most consumer technologies and software. As a result, by the time a facility enters operation, vendors may no longer support the technologies initially selected, including IIoT devices or AI systems. In some cases, companies supplying cutting-edge components may no longer exist.

Off-the-shelf IoT and IIoT devices, such as sensors, pose additional challenges, as they may include minimal cyber security protections. These devices often rely on weak or widely known default passwords, making them vulnerable unless security risks are identified and mitigated. In situations where networking capabilities are undesirable, hardware components enabling connectivity may need to be physically removed.

38 Carrie Gardner, et al., "Contextualizing End-User Needs: How to Measure the Trustworthiness of an AI System", SEI Blog, Carnegie Mellon University, 17 Jul 2023. Available at: https://doi.org/10.58012/8b0v-mq84.

39 Human-in-the-loop refers to the need to have a human actively participating in the operation, supervision, or decision making of an AI-enabled system.

40 Jessica A. Baweja, Corey K. Fallon, and Brett A. Jefferson, "Opportunities for human factors in machine learning", Frontiers in Artificial Intelligence, 20 Apr 2023. Available at: https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2023.1130190/full.

41 IAEA, "Nuclear Security Culture", IAEA Nuclear Security Series, No. 7, 2008. Available at: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1347_web.pdf.

The diversity of vendors involved in producing IIoT and AI components also introduces supply chain risks at multiple points in both the physical and digital lifecycle of each device. Addressing these risks will require coordinated efforts by physical and cyber security personnel, supported by robust validation, verification, and qualification procedures.[42,43]

Safety-Security Interfaces

The primary concern for most nuclear power plants and many other nuclear facilities is the possibility that a malicious actor could disable or manipulate critical safety functions. As digital technologies, including IIoT devices and AI, are incorporated into systems that could, even indirectly, affect safety, the number of potential technological vulnerabilities increases. These vulnerabilities stem not only from system errors but also from the risk of deliberate manipulation intended to trigger a safety event or disrupt facility operations.

Ongoing work is assessing practical approaches to manage these risks. A 2024 joint report by the Canadian Nuclear Safety Commission, the UK Office for Nuclear Regulation, and the U.S. Nuclear Regulatory Commission offers a useful framework for evaluating AI integration from a safety perspective.[44] The framework maps the consequences of AI failure against the level of AI autonomy, illustrating that AI used for low-consequence, non-autonomous functions, such as insight and collaboration, is relatively easy to integrate, while highly autonomous AI in high-consequence safety functions is inadvisable.

Safety-related decision-making software need to undergo rigorous quality assurance to meet regulatory requirements, and any IIoT–AI tool used in this context would be held to the same standards. However, as noted earlier, establishing robust quality assurance methods for AI remains an active area of research. Thus, a sensible approach could be to limit AI to advisory and analytical roles. For example, an AI system with access to comprehensive plant data could help operators by flagging anomalies, identifying likely causes, and assessing their relevance. Nevertheless, such systems remain vulnerable to cyber manipulation, whether to conceal an anomaly or generate a false one. Operators need to therefore be trained to critically evaluate AI recommendations and recognise when outputs may be unreliable.

Conclusions

The previous sections outlined the opportunities and challenges associated with adopting IIoT and AI in the nuclear sector and examined their security-related benefits and costs. From this analysis, five key conclusions emerge.

1. Security resource requirements are critical to include in cost–benefit assessments for IIoT–AI integration. Expected efficiencies or cost savings should be weighed not only against the technologies' direct costs but also against the physical and cyber security measures required for secure deployment. These assessments need to account for a wide range of risks, including data security and data sovereignty, IIoT–AI specific vulnerabilities and attack pathways, and human factors.

2. Retrofitting existing facilities for IIoT–AI integration presents fundamentally different – and often greater – security challenges than incorporating these technologies into new designs. Older facilities were not built to accommodate the hardware, networking, and security requirements of IIoT and AI, making secure integration significantly more complex. This challenge can also apply to "new builds" based on designs finalised decades earlier. In contrast, facilities designed from the outset to incorporate IIoT and AI, especially those that explicitly address associated cyber and physical security requirements, may face a very different security cost–benefit balance.

42 Sarah Case Lackner and Mara Zarka, "Nuclear Security and the Nuclear Supply Chain in the Age of Artificial Intelligence", VCDNP, Apr 2025. Available at: https://vcdnp.org/wp-content/uploads/2025/04/VCDNP_AI-and-Security-of-the-Nuclear-Supply-Chain_web.pdf.

43 IAEA, "Computer Security Approaches to Reduce Cyber Risks in the Nuclear Supply Chain", IAEA, 2022. Available at: https://www-pub.iaea.org/MTCD/Publications/PDF/TDL-011web.pdf.

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

3. As IIoT and AI are further integrated into nuclear facilities, associated cyber security risks will grow and will span the operational, safety, security, and IT domains. Some risks can already be mitigated, while others remain under active development. Cyber risks are expected to grow as IIoT data volumes expand and AI systems are increasingly used to analyse that data. At the same time, AI-enabled capabilities, such as facility-wide anomaly detection, may help counter some of these risks. Broader adoption of IIoT-AI systems will require further progress in AI security, validation, and verification, and model trustworthiness.

4. Data security will become even more important as nuclear facilities further integrate IIoT and AI. As IIoT adoption expands, facilities will generate large volumes of potentially sensitive data. Protecting this data needs to be a priority, requiring appropriate classification, network segmentation, and other security measures, as well as compliance with any national data sovereignty requirements, particularly when cloud solutions are considered. As reliance on AI grows, facilities will also need mechanisms to detect and mitigate manipulation of both training data and operational inputs.

5. Human factors will remain challenging. Given the high-consequence environment of nuclear facilities, most AI systems – especially those informing safety or security decisions – will require a "human-in-the-loop". Staff in this role need to be trained to interpret AI recommendations, understand their limitations, and rapidly judge the validity of AI-generated conclusions.

Consumer IoT, ranging from smart watches to mobile phones to home appliances, and publicly available AI models and systems are becoming ubiquitous.

Consumer IoT, AI Models, and New Risks

In parallel with the industry-specific advances discussed in the previous section, consumer IoT and powerful AI models, such as large language models, are rapidly advancing and becoming ubiquitous. While these technologies offer significant benefits in everyday life, they also have the potential to expand the capabilities of malicious actors. Nuclear security professionals will need to anticipate and mitigate the risks associated with their misuse in relation to nuclear facilities and activities. These risks and potential mitigations are the focus of the current section.

New and Emerging Risks Related to Consumer IoT

An increasing range of everyday commercial products now include built-in IoT capabilities, sometimes without being clearly identified as such. Beyond prominent examples – such as smartwatches, networked cameras, Bluetooth devices, and mobile phones – IoT functions are now found in lighting systems, kitchen appliances, monitors, televisions, and even many medical devices.[45,46,47]

45 A1, "11 IoT examples across different industries," A1 Digital Knowledge Hub, last updated 26 Nov 2025, accessed Nov 2025. Available at: https://www.a1.digital/knowledge-hub/11-iot-examples-across-different-industries/.

46 Pacific Northwest National Laboratory, "The Internet of Things Brings a Web of Promises and Perils to the Smart Grid, Experts Say", DOE Science News Source, Newswise Initiative, 26 Oct 2020. Available at: https://www.newswise.com/doescience/the-internet-of-things-brings-a-web-of-promises-and-perils-to-the-smart-grid-experts-say/?article_id=740548.

47 Chunyan Li, et al., "A review of IoT applications in healthcare", Neurocomputing, Vol. 565, 14 Jan 2024. Available at: https://www.sciencedirect.com/science/article/pii/S0925231223011402.

As IoT technologies become smaller and more commonplace, they can be introduced into a nuclear facility, whether inadvertently or maliciously, without adequate security controls, such as protections against unauthorised external connectivity. These devices may be brought in by unwitting or malicious insiders, delivered by drones, or inserted into the supply chain. Once inside, their wireless networking capabilities can provide pathways for cyberattacks. These modes of introduction mirror challenges faced across many other sectors.

The goals of a cyberattack vary, but commonly include financial gain, data theft, disruption of IT or OT systems, espionage, sabotage, or influence operations. These objectives can be pursued through a range of attack methods, such as disrupting communications, exploiting software vulnerabilities, conducting phishing or social engineering campaigns, delivering and installing malicious software, gaining unauthorised access to sensitive networks, or manipulating data to mislead operators or automated systems.

IoT-enabled components or devices may also be intentionally introduced into facilities without undergoing proper cyber security review. For example, components with undocumented or unsecured wireless capabilities could enter through the supply chain, whether through the substitution of parts by a falsified supplier or through tampering during transit. Grey-market component purchases pose additional risks, as their provenance and security features are often uncertain. Consumer IoT devices embedded in everyday items, such as coffee makers in break rooms, can also introduce unforeseen vulnerabilities if not properly managed. Insecure network access is also a concern. This can occur via personal hotspots or mobile networks, or through wireless networks whose coverage extends beyond the facility's perimeter.

Cyber security professionals understand these risks, but they are difficult, if not impossible, to eliminate entirely. The rapid expansion of IoT capabilities into an increasing array of unexpected devices has amplified the challenge. Many newly IoT-enabled products, such as medical devices, may not be routinely scrutinised for cyber security vulnerabilities. Nonetheless, the most common and persistent risks still stem from familiar consumer IoT devices: smartphones, smartwatches, and similar personal electronics used by staff in nuclear and other high-risk facilities. These devices pose security concerns regardless of whether they are personally owned or company-issued, although robust cyber security measures can and should be implemented to mitigate the associated risks.

Over the past decade, a substantial body of cyber security guidance relevant to nuclear facilities has been developed, including resources explicitly focused on the protection of nuclear material, facilities and information. The IAEA's Nuclear Security Series includes several key publications on computer and information security, such as Computer Security for Nuclear Security (NSS No 42-G),[48] Computer Security Techniques for Nuclear Security (NSS No 17-T)[49] and Security of Nuclear Information (NSS No 23-G).[50] In addition, international standards from the International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO) address cyber security for IoT systems, such as IEC 62443 for industrial and control systems[51], and ISO/IEC 27402[52] and ISO/IEC 27404[53] for consumer IoT, which set baseline requirements for security, privacy, and device labelling.

48 IAEA, "Computer Security for Nuclear Security", IAEA Nuclear Security Series, No. 42-G, 2021. Available at: https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1918_web.pdf.

49 IAEA, "Computer Security Techniques for Nuclear Facilities", IAEA Nuclear Security Series, No. 17-T (Rev. 1), 2021. Available at: https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1921_web.pdf.

50 IAEA, "Security of Nuclear Information", IAEA Nuclear Security Series, No. 23-G, 2015. Available at: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1677web-32045715.pdf.

51 IEC, "Understanding IEC 62443", IEC Blog, 26 Feb 2021. Available at: https://www.iec.ch/blog/understanding-iec-62443.

52 ISO, "Cyber Security — IoT security and privacy — Device baseline requirements", ISO/IEC 27402:2023, Edition 1, Nov 2023. Available at: https://www.iso.org/standard/80136.html.

53 ISO, "Cyber Security — IoT security and privacy — Cyber Security labelling framework for consumer IoT", ISO/IEC 27404:2025, Edition 1, Oct 2025. Available at: https://www.iso.org/standard/80138.html.

Assessing Nuclear Security Risks from Commercial and Open-Source AI

The data-gathering and processing capabilities of current and emerging AI models and systems, particularly large language models and agentic AI, may amplify the risks described above and introduce additional nuclear security concerns. While some of these risks relate to the misuse of IoT and IIoT data, the availability of extensive open-source information is itself a significant vulnerability.

In particular, current and next-generation AI models could enable malicious actors to more effectively gather and analyse open-source data, helping them identify how to target specific nuclear facilities and to decide which facilities to target. AI systems also enhance social-engineering capabilities, enabling more convincing phishing and spear-phishing attempts, as well as more effective insider-recruitment efforts.[54]

AI-driven code generation is becoming increasingly sophisticated, giving less capable malicious actors new opportunities to create and deploy malware and conduct other cyberattacks. When these enhanced capabilities are combined with uncontrolled IoT devices that may provide entry points for malware, the likelihood of a successful attack can increase significantly. Further, if IIoT devices are integrated into nuclear facilities, a compromise could expose streams of sensitive data that an adversary using AI tools could analyse to deepen their understanding of the facility. An attacker could then manipulate and reinsert altered data into the system to advance their objectives, potentially corrupting the conclusions drawn by both human operators and AI systems.
Broadly, many legal and regulatory approaches are being explored to manage the risks of AI beyond the nuclear context.[55] The UN and other international bodies are also examining these risks.[56] Any effort to regulate commercial AI models is likely to involve multiple national and international stakeholders.

Conclusions

1. Cyber security risks to nuclear facilities from increasingly ubiquitous consumer IoT devices are evolving but not new, and reliable guidance already exists. Relevant computer security guidance for nuclear security is available from the IAEA, and IoT and cyber security standards developed by organisations such as ISO and IEC are also applicable to many situations in the nuclear sector.

2. Most electronic items brought into facilities should be inspected, including those not previously considered security concerns. As IoT capabilities become ubiquitous, many consumer devices and off-the-shelf components used in facilities may include networked functions. Medical devices, some of which cannot be removed, are also increasingly equipped with these capabilities.

3. Publicly available AI systems are becoming increasingly capable and, when combined with data from IoT or IIoT devices, could significantly enhance a malicious actor's capabilities. IoT and IIoT devices in facilities can expose large volumes of sensitive data if misused or compromised. AI models can enable adversaries to analyse this data, derive operational insights, and design cyberattacks targeting these devices, including attacks that manipulate the data they produce.

54 Sarah Case Lackner and Zaheed Kara, "Artificial Intelligence and Nuclear Security Governance: Addressing the Risks of Frontier AI", VCDNP, Dec 2025. Available at: https://vcdnp.org/wp-content/uploads/2025/12/VCDNP_AI-and-Nuclear-Security-Governance_web.pdf.

55 These include regional, national, and sub-national laws and proposals on AI governance and safety, including the EU Artificial Intelligence Act, several laws in the U.S. State of California, including SB-53 – Transparency in Frontier AI Act, and the proposed Artificial Intelligence and Data Act under consideration in Canada.

56 Such as, for example, the formation of the High-Level Advisory Body on Artificial Intelligence and its Final Report "Governing AI for Humanity" (Sep 2024), and the recent establishment of two AI governance bodies: The Global Dialogue on AI Governance and the Independent International Scientific Panel on AI. For more details, see https://www.un.org/en/ai-advisory-body and https://www.un.org/en/delegate/two-new-mechanisms-promote-cooperation-ai-governance.

4. The ubiquity of commercial IoT and AI makes it impossible to eliminate all related cyber security risks. Some devices, such as medical equipment, cannot be fully controlled, and IoT-enabled components are increasingly likely to enter facilities unnoticed. Meanwhile, advancing AI models are expanding the capabilities available to malicious actors.

As digital technologies increasingly enter the nuclear sector, it will be useful to learn from other energy and critical infrastructure sectors that more rapidly adopt these technologies.

Recommendations

Four recommendations are offered for nuclear security professionals, outlining areas for further analysis and dialogue on IoT, AI, and nuclear security. The recommendations are directed primarily at decision-makers, regulators, and international organisations.

1. In highly digitalised nuclear facilities using IIoT and AI, nuclear security, especially cyber security, should prioritise reliability and resilience over the unrealistic goal of preventing every attack.

As noted in the conclusions from both of the previous sections, it is likely to be impossible to prevent all of the broad and expanding range of cyberattacks that are likely to be levelled against nuclear facilities in the future, due in large part to the expanding use of AI and IoT in nuclear facilities and by malicious actors. Further, the use of AI systems in nuclear facilities introduces novel risks, some of which will be difficult to eliminate due to the "black box" functioning of many AI models.

When preventing the attack is impossible, the emphasis should shift to preventing the worst-case consequences and responding to the attack to maintain the functioning of the facility. Two concepts that can be considered within the nuclear security framework of prevention, detection, and response are helpful in framing this:

- **Reliability:** Eliminating opportunities for digital systems to affect fundamental safety functions via passive safety systems and other engineering features, and managing the remaining risks through robust cyber security measures.

- **Resilience:** ensuring that facilities can return to safe, stable operation quickly after an incident, as a key part of the response to an incident.

At the same time, the graded approach to nuclear security and defence-in-depth remain essential, as well as nuclear security and cyber measures to manage the remaining risk via protection against, detection of, and response to threats.

2. Cost-benefit assessments for IIoT and AI integration should account for physical and cyber security measures needed to maintain robust nuclear security when these technologies are used. These assessments should account for a wide range of risks, including data security and data sovereignty, IIoT and AI-specific vulnerabilities and attack pathways, and human factors. Further, as retrofitting existing facilities for IIoT and AI integration presents fundamentally different – and often greater – security challenges than incorporating these technologies into new designs, the risk-benefit calculation for new designs and for existing facilities is likely to differ.

3. The nuclear sector should proactively learn from other critical infrastructure sectors that are advancing more rapidly in digitisation and in the use of IIoT and AI. Different parts of the energy sector, and critical infrastructure more broadly, are already confronting challenges the nuclear industry has yet to face. Policymakers should seek opportunities to establish mechanisms for systematic knowledge-sharing with these sectors, drawing on their experience to strengthen nuclear security and avoid repeating preventable mistakes.

The nuclear sector is not alone in confronting the rapidly evolving challenges and opportunities presented by IoT and AI. However, because it has adopted new technologies more slowly than many other critical infrastructure sectors, there is an opportunity to learn from their experience. Exchanges with these sectors could be particularly valuable in areas such as:

- Defining the qualifications and roles of a "human-in-the-loop" for high-consequence industries.
- Managing data security and data sovereignty requirements.
- Establishing the trustworthiness of AI systems and qualifying IIoT for high-consequence applications.

At the same time, the nuclear sector's high-consequence nature and stringent regulatory environment mean that lessons from other sectors need to be adapted carefully. Any proposed solutions will need to be evaluated through a nuclear-specific lens and tailored to the unique requirements of nuclear facilities and activities.

4. Up-to-date, practical guidance for operators and regulators on maintaining nuclear security in a rapidly changing environment should be continuously developed and shared by international and other relevant organisations, including NGOs and industry groups. New security challenges arising from AI and its links to IoT are evolving faster than current international and national advice and information can address. Existing mechanisms for issuing regulations and guidance at the national and international level often struggle to keep pace with technological developments, making more agile approaches essential.

The IAEA in particular is working to meet the needs of operators and regulators for assistance in this rapidly evolving area. Their efforts include not only technical publications and training courses but also dedicated convenings on nuclear security and AI,[57] as well as Coordinated Research Projects.[58] Webinars and virtual workshops offered by the IAEA[59] and by organisations such as the World Institute for Nuclear Security also help address emerging needs.[60]

However, the demand for information is skyrocketing, and new questions continue to arise. Regulators, operators, and other stakeholders would benefit from reliable guidance in areas such as:

- Classification of information for AI and IIoT
- Security implications of using AI and IIoT for decision-making support in nuclear power plants
- Insider risks and human factors associated with AI and IoT
- Security considerations for "human-in-the-loop" approaches
- Verification and validation of AI systems deployed in nuclear facilities

Where to Go from Here?

The digital transformation that began in the 1980s and 1990s marked a significant shift for nuclear security and the nuclear sector as a whole. By the early 2000s, it was clear that cyber security was essential not only for protecting information technology but also for safeguarding operational systems. This required an evolution in nuclear security, from a framework centred on "guns, gates, and guards" to one that integrates robust cyber security measures. Although initially met with resistance, this integration is now widely recognised as indispensable.

The sector is now approaching another paradigm shift driven by AI and IoT. In a classic dual-use dilemma, these technologies offer new opportunities for operational insight and automation, but they also create novel pathways for malicious actors. Existing nuclear security thinking may need to shift to adapt to this changing threat: for example, with a renewed focus on reliability and resilience.

Looking ahead, maintaining strong nuclear security for both ageing facilities and new builds will require learning from the challenges being faced in the current transition and being ready to apply those lessons to better manage future transitions. By understanding the successes and failures in managing this paradigm shift, and by considering how past paradigm shifts were managed, the nuclear security community will be better prepared for the next transformation, which is certain to come.

57 IAEA, "Technical Meeting on the Application of Artificial Intelligence for Nuclear Security" IAEA EVT2405595, 20 – 24 Oct 2025. More information available at: https://www.iaea.org/fr/node/205801.

58 IAEA, "Enhancing Computer Security of Artificial Intelligence Applications for Nuclear Technologies", Coordinated Research Projects Call for Proposals, approved date 30 Apr 2025. More details available at: https://www.iaea.org/projects/crp/j02024.

59 Including the IAEA's "Innovation in Action: Real-World Applications in Nuclear Power" webinar series and the "Webinar Series on Nuclear Security – Looking Beyond ICONS 2024", which both cover new technologies and their implications for the nuclear sector.

60 World Institute for Nuclear Security, "Exploring the Role of Artificial Intelligence in Strengthening the Security of Nuclear Facilities", WINS Virtual Workshop, 10 – 11 Dec 2024. More information available at: https://www.wins.org/event/7901/wins-virtual-workshop%3A-exploring-the-role-of-artificial-intelligence-in-strengthening-the-security-of-nuclear-facilities.

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