VCDNP Vienna Center for Disarmament and Non-Proliferation

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

January 2026

The Internet of Things and the Impact on Nuclear Facilities

Donald D. Dudenhoeffer

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

Author

Donald D. Dudenhoeffer is a Senior Cyber Security Consultant with over 35 years of experience in nuclear operations and security. He currently serves as a Cyber Security Consultant supporting the commercial nuclear sector at the Barakah Nuclear Power Plant in Abu Dhabi, UAE, while also contributing as a part-time researcher at the Austrian Institute of Technology (AIT).

Previously, Mr. Dudenhoeffer held the position of Senior Information Technology Officer in the Division of Nuclear Security (NSNS) at the International Atomic Energy Agency (IAEA), where he led the Computer Security Program. In this role, he provided guidance and support to Member States in developing robust cyber security frameworks for their nuclear facilities.

He holds a Master of Science degree in Operations Research from the US Naval Postgraduate School and is a qualified nuclear engineer.

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 Internet of Things provides previously isolated industrial items and machines with access to data streams.

Introduction to the Internet of Things (IoT)

History of Industry Transformation

Technology innovation constantly shapes the world and work processes. In the 1900s, the world was undergoing a transformative era marked by the rise of electricity, the proliferation of telephones, the emergence of the automotive industry, and significant advancements in manufacturing technologies.

Over the course of 125 years, we have witnessed a remarkable transformation – from automobiles being a luxury reserved for the privileged few to becoming a widespread commodity, with an estimated 1.45 billion cars in use globally (2022).[1] The automobile continues to evolve – from a human-operated experience to one increasingly defined by autonomous features, including self-driving capabilities in certain models. The telephone has also evolved dramatically – from a shared landline device reliant on party lines for basic human communication to today's ubiquitous mobile phones with an estimated 8.58 billion mobile subscriptions globally, surpassing the world's population of 7.95 billion (2022).[2]

The automobile and telephone are two examples of transformative technologies that have dramatically evolved in both design and function over the past 125 years and continue to do so.

1 David Bonnici and Mike Stevens, "It's 2024, how many cars are there in the world?", Which Car? by Wheels, 09 Feb 2024. Available at: https://www.whichcar.com.au/news/how-many-cars-are-there-in-the-world.

2 Felix Richter, "Charted: There are more mobile phones than people in the world", World Economic Forum, 11 Apr 2023. Available at: https://www.weforum.org/stories/2023/04/charted-there-are-more-phones-than-people-in-the-world/#:~:text=According%20to%20the%20International%20Telecommunication,billion%20halfway%20through%20the%20year.&text=2016%20was%20the%20year%20mobile,Image%3A%20Statista.

Myriad other innovations have emerged in this time, and many others have become obsolete. Technological progress drives not only evolution but also convergence. Today, for example, smartphones and other digital devices are increasingly integrated into automotive systems, enabling a wide array of features such as navigation, location tracking, vehicle diagnostics, and performance monitoring.[3] It is such a convergence of technologies that has led to a rise in network-enabled devices, also known as the "Internet of Things" (IoT).

On the consumer level, IoT is the collection of networked physical devices, such as automobiles or home appliances, that share information and interact with each other. This paper explores the integration of such systems into industrial processes, specifically in ways relevant to its application in nuclear power plants (NPPs). Rather than focusing on the technical specifications of IoT, the discussion highlights the paradigm shift IoT introduces to work processes and nuclear plant operations. The objective is to present a pragmatic perspective on how IoT can be applied to both current and future generations of nuclear power plants.

Industrial Internet of Things

IoT systems offer both a technological framework for communication and a shift in operational paradigms, enabling data-driven connections and interactions between previously isolated digital objects. These "things" gain access to remote data streams, applications, cloud workloads, and functionalities, fostering interconnectivity with other devices and systems. As a result, previously standalone devices can now become part of dynamic, intelligence-driven, and interdependent systems that enhance visibility and transform operations.

This has led to the emergence of the concept of Industrial Internet of Things (IIoT). The term IIoT, attributed to General Electric in 2012, is the application of IoT technologies (e.g. sensors, devices, applications, and associated networks) to support industrial operations, especially in the manufacturing sector.[4] Another way of saying this is that IIoT is an ecosystem consisting of a vast array of devices, sensors, applications, and associated networks that collaboratively work together to collect, monitor, and analyse data in order to support industrial operations.[5]

The ability to capture and share information related to equipment and process performance across a range of distributed applications, enabled by IIoT, has provided tremendous opportunities for increasing efficiency and work planning. Just as you can use your mobile phone to access smart car features, imagine accessing real-time plant performance data or directing nuclear plant operations from your phone. This would represent a dramatic shift in how operations are conducted.

In today's industrial landscape, terms like consumer based IoT, IIoT, Industry 4.0, and Smart Factories are commonly used to describe the integration of technologies and the transformation of industrial/manufacturing processes. Focusing on the labels is less useful than understanding the key characteristics of this transformation, including:

- **High Connectivity:** Devices, sensors, and systems are interconnected via industrial-grade networks that support real-time data exchange across systems and locations.
- **Sensor Rich:** Sensor networks support access to an array of equipment and plant parameters.
- **Real-Time (Monitoring & Control):** Industrial processes are continuously observable, with instantaneous feedback mechanisms supporting swift adjustments and adaptive control.
- **Data-Driven:** Operations are supported by continuous data collection and analysis to inform decision-making.

3 Yoav Bar-Nov, "Connected Cars: Exploring the Intersection of Automotive and IoT", AllStarsIT, accessed Oct 2025. Available at: https://www.allstarsit.com/blog/connected-cars-exploring-the-intersection-of-automotive-and-iot.

4 Hugh Boyes et al., "The industrial internet of things (IIoT): An analysis framework", Computers in Industry, Vol. 101, Oct 2018, pp.2-3. Available at: https://www.sciencedirect.com/science/article/pii/S0166361517307285#bbib0025.

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

- **Heterogenous Interaction:** A diverse collection of data, systems, and applications are able to communicate and interact with each other.
- **Edge & Cloud Computing Integration:** Data is processed locally (edge computing) for speed and efficiency, or in cloud platforms for large-scale analytics, storage, and remote access.
- **Artificial Intelligence (AI):** Plant data is used in AI systems for data analysis, human decision support, and where appropriate, autonomous action.
- **Levels of Automation in Operation:** Machines can make decisions and adjust operations with varying degrees of human oversight.

Core IIoT Components and Architecture

The core IIoT architecture is a layered framework designed to facilitate the aforementioned characteristics. Figure 1 illustrates a high-level conceptual view of the IIoT structure. On the left hand side the four key layers are listed (perception, network, processing and application layer) and from the processing layer, two key strategies for managing the data are indicated (edge and cloud computing). Each of these elements are described in more detail below.

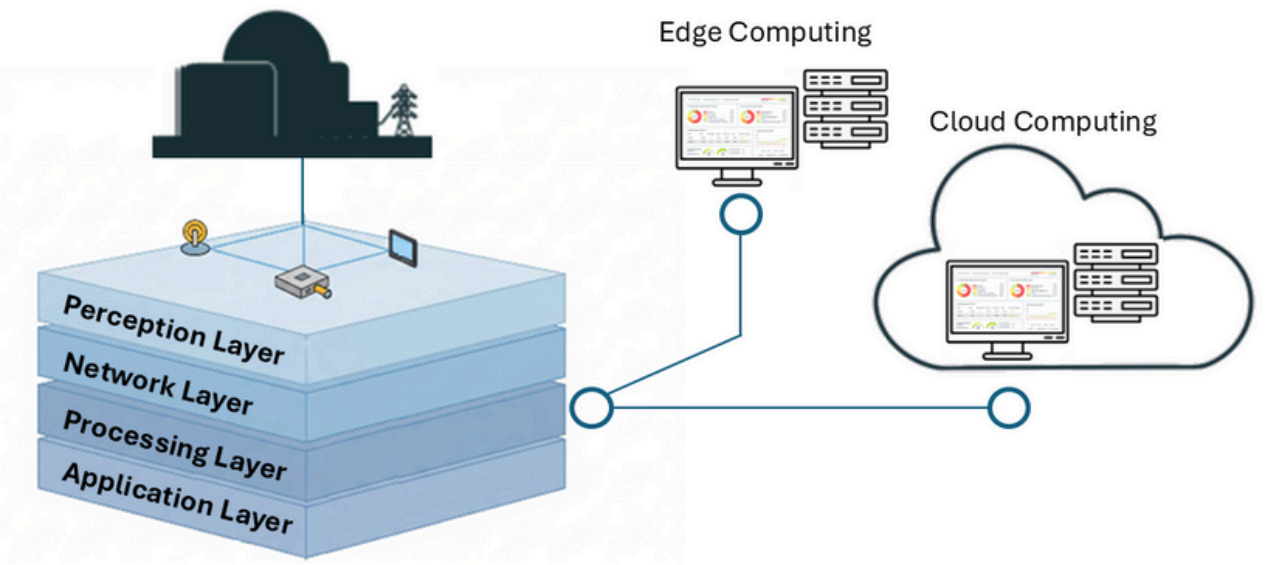


Figure 1: IIoT Framework Overview

Perception Layer / Edge Sensing Layer

Access to meaningful and actionable data is key to an effective IIoT framework. The Edge Sensing Layer consists of the sensors, actuators, devices, processes, and systems from which meaningful real-time data can be collected, for example, data which reflects a specific aspect of a nuclear power plant operation. The IIoT use-case will determine the type and granularity of the data. While most data will come from the existing processes and equipment, some cases may require additional sensors or software applications to obtain (collect or generate) the needed information. Data should be collected with purpose, not just because it can be collected, as indiscriminate collection can impact plant performance, increase cloud infrastructure resource consumption, and raise costs associated with application uses such as Large Language Model (LLM) inference.

Network Layer / Communication Layer

IIoT is characterised by high connectivity. Accessing and communicating plant data to other “things” is necessary. Various communication layers exist to extract data from the Edge Sensing Layer, allowing transport of the data for external use. Ideally, edge data can be extracted from an existing data network or access point. IIoT implementation can become problematic if the current NPP network connectivity does not support data extraction.

Examples include the lack of SPAN/TAP[6] ports available for traffic monitoring or when data networks are strictly segregated from external access. Likewise, new cabling may face a realm of engineering challenges, and the use of wireless technology presents its own set of challenges at an NPP.[7] 5G technologies may help create local networks of sufficient reach and speed to support data collection. However, the deployment of 5G within nuclear facilities must account for radio frequency (RF) restrictions and electromagnetic compatibility (EMC) requirements inside protected areas. In practice, using secure private LTE/5G networks with strict zoning and access controls is an option for managing these constraints.

Once a pathway to the source is established, data transmittal for storage, processing, and application would be conducted over standard or dedicated communication infrastructure.

Depending on the size and nature of the data, IIoT storage infrastructure may need to manage a larger volume of data from the Edge Sensing Layer. A well-conceived data management strategy is needed to effectively use collected data.

Data Processing / Computing Layer

An IIoT framework is implemented to leverage data fusion, analysis, and action across both internal and external objects, i.e. "things". Raw data will likely undergo multiple levels of processing, filtering, analytics, and decision-making to extract meaningful insights or drive actions. Data processing can also help reduce large volumes of data into smaller, meaningful elements, thereby reducing transmission and storage requirements. Data processing may be incorporated at multiple levels. Two non-exclusive strategies have emerged: edge computing and cloud computing. IIoT frameworks may employ elements of both strategies, for example, data could be pre-processed with edge computing to extract relevant features prior to transmittal for use by cloud services.

Application Layer

While the first three layers provide the core infrastructure for making data accessible – extracting, transmitting, and processing data – the fourth layer transforms the data into actionable information to meet meaningful business objectives. Here, for example, data from the NPP, potentially integrated with other data sources, is analysed to enhance situational awareness, provide decision support, and/or automate actions. Applications may also leverage technologies such as AI and digital twins to meet specific business use cases. The Application Layer may communicate information and action back to NPP edge, control, or decision processes.

Business Layer

An essential element of the IIoT framework not illustrated in Figure 1 is the Business Layer. This layer addresses the business viewpoint and associated interests in implementing the IIoT framework. A sound business strategy and cost-effective implementation use-cases are essential for IIoT programme success and sustainability. Key areas include, but are not limited to:[8]

- **Business Vision:** Goals, use cases, and cost-benefit analysis for implementing the IIoT framework.
- **Contracts:** Agreements and contracts related to procurement, operations, and maintenance of the IIoT framework.
- **Regulatory Compliance:** Alignment and compliance with national laws, regulations, and standards.
- **Governance:** Policy, procedures, and structures to implement and manage the IIoT system and associated processes.

6 SPAN (Switched Port Analyzer) and TAP (Test Access Point) ports are used to monitor network traffic by copying data from one part of the network and sending it to a monitoring system.

7 Arto Laikari and Jere Backman, "Industrial Internet of Things in Nuclear: Feasibility Study", Energiforsk, Report 2021:726, pp. 23-26. Available at: https://energiforsk.se/media/29219/industrial-internet-of-things-in-nuclear-energiforskrapport-2021-726.pdf.

8 Industry IoT Consortium, "The Industrial Internet Reference Architecture", An Industry IoT Consortium Foundational Document, Version 1.10, 07 Nov 2022, pp. 17-18. Available at: https://www.iiconsortium.org/wp-content/uploads/sites/2/2022/11/IIRA-v1.10.pdf.

Key Technologies Enabling IIoT in Industrial Settings

IIoT has become practical and commercially viable through the convergence of advanced communication, computing, and sensing technologies that enable the high-speed transmission, storage, and analysis of large-scale industrial data.

5G and Advances in Communication Technology

The foundational principle of IIoT is the communication between interconnected devices. The emergence of 5G mobile networks has accelerated IIoT adoption by providing faster, more reliable, and ultra-low-latency connectivity between interconnected devices and systems. Engineered features and capabilities provided by 5G that enable IIoT include:

- Enhanced Mobile Broadband: Speeds exceeding 10 Gbps
- Ultra-Reliable Low Latency Communications
- Massive Machine-Type Communications: Supporting up to 1 million devices per square kilometre
- Network Slicing: Creating multiple virtual networks running a single shared physical infrastructure

Ongoing research efforts are focused on next-generation 6G communication networks and using cutting-edge technologies, such as AI, to achieve faster speeds and improved network performance.[9]

Edge Computing

Edge devices are essential, as they produce telemetry data which are transmitted to other IIoT systems for analysis or action. However, the amount of telemetry data produced by sensors can be overwhelming. One energy utility reported "over 1.8 billion sensor values were being recorded daily from a single fleet of energy assets."[10]

Edge computing processes data close to the source of data generation. By enabling local pre-processing, on-premises analysis, and selective data transmission, edge computing reduces latency. Further, by condensing data to only relevant information it minimises data transmission and storage demand, whether on-site or in the cloud. Moreover, it can prevent sensitive data from being uploaded to the cloud.

Cloud Computing

Cloud computing relies on centralised data centres to store and process large volumes of data. It plays a pivotal role in enabling and scaling IIoT systems by providing flexible, scalable, and cost-effective infrastructure and services. Notably, cloud platforms can provide the data storage infrastructure to collect and process massive volumes of data generated from edge devices and connected systems.

While edge computing addresses computational tasks that require low latency or proximity to the data source, cloud computing offers a broad spectrum of analytical capabilities through various service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Cloud platforms such as AWS IoT Greengrass and Azure IoT Edge facilitate edge intelligence and long-term analytics, while services such as AWS IoT Core and Azure IoT Hub provide device management and orchestration.

9 Ericsson, "6G Networks", accessed Oct 2025. Available at: https://www.ericsson.com/en/6g.

10 IIoT World, "Energy's Silent Challenge: The Operational Bottlenecks of Data Volume, Not Data Access", 22 Jul 2025. Available at: https://www.iiot-world.com/energy/renewable-energy/energy-data-overload-bottleneck/.

Big Data and AI

AI models and systems are both enablers of IIoT and applications for IIoT. As IIoT edge devices can generate significant quantities of data, AI models and systems are valuable in performing big data analysis on this sea of data. In other words, AI models and systems can use machine learning to process and analyse the massive amounts of data generated by IIoT devices, extracting valuable insights. This analysis can be conducted either on edge computing or by external resources via cloud computing.

AI can also support the use of IIoT infrastructure by optimising network traffic. Self-Organizing Networks (SONs) are an example of an application of AI technologies to configure, optimise, and heal data networks when new equipment is added or network failures occur.

The Advanced Power Reactor 1400 is a Generation III+ reactor design, developed in South Korea. One example of this design is Unit 4 of the Barakah Nuclear Energy Plant in the United Arab Emirates. Credit: Emirates Nuclear Energy Company.

Understanding IIoT in the Nuclear Context

Nuclear Power Industry Evolution

On 20 December 1951, the Experimental Breeder Reactor (EBR-1) near Arco, Idaho, became the first nuclear reactor to produce usable electricity, enough to power four 200-watt lightbulbs.[11] The Obninsk APS-1 plant in the Soviet Union soon followed suit in June 1954, providing 5 megawatts of electricity to the power grid.[12] The late 1950s and 1960s saw the design and operation of commercial power reactors around the world: France in 1959, the United States of America in 1960, Canada in 1962, and the Soviet Union in 1964, starting the nuclear power industry.

Since then, the nuclear technology base has continued to advance, evolve, and transform. Reactor plant technology transformation is nominally grouped in generations:[13]

- Generation I: Early Prototype Reactors
- Generation II: Commercial Power Reactors
- Generation III (III+): Advanced Light Water Reactors

11 US Department of Energy, "9 Notable Facts About the World's First Nuclear Power Plant - EBR-I", Office of Nuclear Energy, 18 Jun 2019. Available at: https://www.energy.gov/ne/articles/9-notable-facts-about-worlds-first-nuclear-power-plant-ebr-i.

12 Paul R. Josephson, "Red Atom: Russia's Nuclear Power Program from Stalin to Today", University of Pittsburgh Press, 2005, p. 2. ISBN 978-0-8229-7847-3.

13 Stephen M. Goldberg and Robert Rosner, "The History of Reactor Generations", American Academy of Arts and Science, 2011, pp. 3-7. Available at: https://www.amacad.org/publication/nuclear-reactors-generation-generation/section/5.

- Generation IV: New and advanced reactor technologies:[14]

  a. Gas-cooled fast reactor
  b. Lead-cooled fast reactor
  c. Molten salt reactor
  d. Sodium-cooled fast reactor
  e. Supercritical water-cooled reactor
  f. Very high-temperature gas reactor

In addition to the above categorisation, the term "advanced reactors" is often used to group together non-light water reactor designs and small modular reactors.[15]

Since the 1990s, the level of digitalisation has also advanced. The use of analogue instrumentation and control has gradually given way to computer-based technology and digital components. This digital transformation continues to grow, albeit at a slower pace than many non-nuclear industries.

The average age of the current fleet of nuclear power plants is 32 years, with life extension programmes for many pushing effective operations up to 60 to 80 years.[16] Newly commissioned NPPs have a significantly different digital footprint than their predecessors. Where an older plant may have a digital footprint of hundreds of devices, a modern plant may encompass thousands.

This paper focuses on IIoT integration at a contemporary Generation III light water reactor and will use the APR1400 (Advanced Power Reactor 1400) pressurised water reactor (PWR) design as an illustrative example, although other designs such as the AP1000, EPR, VVER-1200, HPR1000, or ACPR-1000 could likewise have been used.

The APR1400 is a Generation III+ PWR developed by Korea Electric Power Corporation and Korea Hydro & Nuclear Power. It is a flagship export design currently commissioned in the Republic of Korea and the United Arab Emirates, with additional sites designated for construction in Czechia. The design of the APR1400 started in 1992. Standard Design Approval from the US Nuclear Regulatory Commission (USNRC) occurred in 2018, with full Design Certification in 2019. The latest commission of the APR1400 Unit was Barakah Unit 4 in the United Arab Emirates, which commenced commercial operation on 5 September 2024. This underlines that even the most recent commissioned plants are based on designs that may be 15 to 20 years old, predating many IIoT concepts and the associated enabling technologies. IIoT was simply not a concept of operation when currently operating Gen III/III+ reactors were designed.

Nuclear Power Plant Control Architecture

The instrumentation and control (I&C) infrastructure at an NPP is essentially the nervous system that keeps the plant and its system functioning. The I&C system would also likely serve as the primary source of Edge telemetry data, if IIoT were integrated in an NPP.

The current fleet of nuclear power plants predominantly uses a distributed control system (DCS) architecture for I&C. In a DCS, control is proximal to the actual physical processes being managed, such as reactor control, steam plant management, and electrical power generation. An alternative to the DCS structure is the supervisory control and data acquisition (SCADA) architecture in which monitoring and control are exerted over a large geographic area. Examples of SCADA usage include controlling a gas pipeline or an electric power grid.

14 World Nuclear Association, "Generation IV Nuclear Reactors", updated 30 Apr 2024. Available at: https://world-nuclear.org/information-library/nuclear-fuel-cycle/nuclear-power-reactors/generation-iv-nuclear-reactors.

15 US Nuclear Regulatory Commission, "Advanced Reactors", 04 Mar 2025. Available at: https://www.nrc.gov/reactors/new-reactors/advanced.html.

16 Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, "Nuclear energy worldwide 2024", 15 Feb 2024. Available at: https://www.grs.de/en/news/nuclear-energy-worldwide-2024.

Nuclear power plants are designed for site-based operations, with minimal or no external connectivity. Remote operations of safety and control systems are not supported by design. Furthermore, production systems (e.g. reactor control, safety, and plant operations) are kept strictly separate from enterprise IT systems. This architectural separation is commonly referred to as the "island" concept, reflecting the intentional isolation of nuclear control networks from external networks.

The DCS itself can be described at a high level using the Purdue model, which provides a functional representation of the layers and interactions between operational technology (industrial controls) and information technology (business) environments. The Purdue model, illustrated in Figure 2 below, describes the six network levels (level 0 to 5) within an environment and the accompanying systems and technologies within each level.

<table>
<tr><td rowspan="2">Enterprise Zone</td><td>Level 5: Enterprise Business Operations
• Services supporting individual business units and users
• Nominally located at corporate headquarters or potentially cloud based</td></tr>
<tr><td>Level 4: Plant (Site) Planning and Logistics
• At site operational support processes
• Connected to the Enterprise Network</td></tr>
<tr><td colspan="2">Decoupled of Controlled Communications between Zones</td></tr>
<tr><td rowspan="4">Manufacturing / Production Zone</td><td>Level 3: Plant Supervisory and Operations Control
• Workflow management - monitoring, supervisory, and operational control</td></tr>
<tr><td>Level 2: Area/Local Supervisory
• Dedicated control for production systems
• Highly couple and independent (standalone) systems
• Use ranging from 24/7 to situational operation</td></tr>
<tr><td>Level 1: Local Controller
• Devices and systems to provide control of a process</td></tr>
<tr><td>Level 0: Field Devices
• Sensors and actuators interact with low-level controllers
• Physical and logical attributes monitored, physical processes controlled</td></tr>
</table>

Figure 2. Purdue Enterprise Reference Architecture for an NPP, adapted from Stephen Mathezer (2021)[17]

Each of the levels illustrated in Figure 2 represents a potential interface for IIoT interaction, whether for monitoring (data collection), control (an actuating function), or decision support. The Purdue model is a simplistic representation and merely illustrative. A nuclear power plant will contain hundreds of individual systems that are tightly, loosely, or disjointly coupled in control and operation. These systems may provide functions categorised as:

- Safety Related
- Important-to-Safety
- Non-Safety Related
- Security
- Emergency Preparedness
- Support Systems

17 Adapted from Stephen Mathezer, "Introduction to ICS Security Part 2", SANS, 16 Jul 2021. Available at: https://www.sans.org/blog/introduction-to-ics-security-part-2.

The accessibility of a system, i.e. the ability to connect to and extract data from the system's data stream, is often dependent on the function the system is providing as this will dictate security requirements and communication restrictions.

NPP operations are complex, and the number of systems required for operations is numerous. Table 1 lists typical systems that provide safety related functions at a pressurised water reactor nuclear power plant.

Air Compressors Main Control Board Radiation Monitoring System Auxiliary Feedwater System Auxiliary Relay Cabinets Chemical and Volume Control Component Cooling Water Containment Cooling System Containment Isolation Valves Containment Liner-Penetration Containment Pressure/Leak Det	Containment Spray System Containment System Diesel Fuel Oil System Diesel Generator System Diesel Lube Oil System Starting Air System Emergency Service Water System Essential Chilled Water Excore Nuclear Instrument High Head Safety Injection Incore Nuclear Instrument	Instrument Air System Isolation Cabinets Main Steam System Process Instrumentation Passive Safety Injection Pressurizer Reactor Coolant Pump and Motor Reactor Coolant System Reactor Protection System Reactor Vessel and Internals

Table 1. Typical Safety Related Systems at a PWR[18]

Systems may support one or more modes of reactor operation as described in Table 2. Outside of its designated mode of operation, the system may be offline or in a standby mode.

Mode	Title	Mode	Title
1	Power Operation	4	Hot Shutdown
2	Startup	5	Cold Shutdown
3	Hot Standby	6	Refuelling

Table 2. NPP Modes of Operations[19]

The concept of IIoT can be explained beyond Power Operation use and its applications can be examined in other modes of plant operation. For example, while prohibited during Power Operation, connectivity to remote resources may be permitted to support key maintenance activities when the plant is shutdown. Consider the use of a robotic dog to remotely assay the facility for radiation levels or signs of steam leakage. This represents not only a proposed use case, but one that has been realised in actual implementation practice.[20]

18 Nuclear Energy Institute (NEI), "Identifying Systems and Assets Subject to the Cyber Security Rule", NEI 10-04 Rev. 2, Jul 2012, pp. A1-A2. Available at: https://www.nrc.gov/docs/ml1218/ml12180a081.pdf.

19 U.S. Nuclear Regulatory Commission, Standard Technical Specifications: Westinghouse Plants, Rev 5.0, Vol 1. NUREG-1431, Sep 2021, p. 1.1-8. Available at: https://www.nrc.gov/docs/ML2125/ML21259A155.pdf.

20 Sellafield Ltd, "Sellafield robotics: Using spot more for spotless nuclear clean-up", 23 Mar 2023. Available at: https://www.gov.uk/government/news/sellafield-robotics-using-spot-more-for-spotless-nuclear-clean-up. See more examples at: (1) BBC, "Robot dog flips crane switch at nuclear site", 09 Apr 2025. Available at: https://www.bbc.com/news/articles/cn4j833zkqwo. (2) Mikayla Kreuzberger, "Spot the robot dog helps humans inspect nuclear power plant", Duke Energy, 06 Apr 2022. Available at: https://illumination.duke-energy.com/articles/spot-the-robot-dog-helps-humans-inspect-nuclear-power-plant. (3) Canadian Nuclear Laboratories, "Robot dog surveillance in Chalk River legacy fuel storage rod bays", 03 Mar 2025. Available at: https://www.cnl.ca/robot-dog-surveillance-in-chalk-river-legacy-fuel-storage-rod-bays/.

Defensive Strategy and Model

A key aspect of a cyber security programme at a nuclear facility is the implementation of a defensive strategy to guide cyber security controls. The defensive strategy is developed based on recognition of the nature of the threat, the digital assets to be protected, the consequences of compromise, and the available security controls.[21]

The defensive strategy will nominally use a defensive model as the methodology for implementing cyber security controls across the plant control architecture. The defensive model relies upon the main security principles of defence-in-depth and applies a graded approach to protecting digital systems and associated digital assets. A common element of defensive models in the nuclear industry is the use of isolated or "island" facility networks. Defensive models that are frequently used in the nuclear industry include the USNRC trust model[22] and the International Atomic Energy Agency (IAEA) zone and level model.[23] The International Electrotechnical Commission (IEC) Standard 62443 also describes a similar zone and level model which creates groups based on protection against progressive levels of threat.[24]

Each model groups equipment and systems into zones based on their importance to safety, security, and operations, respectively. Strict control sets, defined as security levels, dictate the respective security measures for each zone.

Security levels provide progressively more stringent layers of protection based on the importance of the zone being protected. Systems providing safety/important-to-safety functions are the most important, followed by physical protection functions, plant control functions, business functions, and so on. Important to the application of IIoT technologies is understanding how such models manage and restrict communication between zones.

Defensive models nominally include tightly controlled communication requirements between the different zones (or layers) in the model, often enforced through unidirectional gateways (data diodes) or brokered historians,[25] which allow secure transfer of selected data without exposing higher-importance networks to external access. This often entails isolating facility systems from external communications, such as the internet, and limiting communications to one-way paths from the zones of greater importance to those of lesser importance.[26]

I&C networks within the plant are built to maximise performance often without great consideration for cyber security. As a result, systems are assembled under an assumption of full trust amongst components, i.e. all communications and entities on the network are fully trusted without authentication or encryption requirements. This reduces system complexity and latency. Thus, system isolation from external networks/processes is a key feature to minimise the risk of compromise by an untrusted entity. A key challenge for IIoT implementation in I&C systems is that this defensive model may be at odds with the high connectivity requirements of IIoT frameworks.

21 World Institute of Nuclear Security (WINS), “Cybersecurity in the Nuclear Industry”, 2024, p. 16. Available at: https://www.wins.org/document/cybersecurity-in-the-nuclear-industry/.

22 U.S. Nuclear Regulatory Commission (USNRC), Cybersecurity Programs for Nuclear Power Reactors, Regulatory Guide 5.71, Rev. 01, Feb 2023, pp. 24-26. Available at: https://www.nrc.gov/docs/ML2225/ML22258A204.pdf.

23 International Atomic Energy Agency (IAEA), Nuclear Security Series No. 42-G, Computer Security for Nuclear Security, 2021, pp. 13-16. Available at: https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1918_web.pdf.

24 International Electrotechnical Commission (IEC), “Understanding IEC 62443”, IEC Blog, 26 Feb 2021. Available at: https://www.iec.ch/blog/understanding-iec-62443.

25 A brokered historian in a control network is an architectural approach where process data from industrial processes is collected into a central “historian” database through an intermediary broker service, rather than direct connections. This improves security by limiting direct access to the historian database.

26 International Atomic Energy Agency (IAEA), Nuclear Security Series No. 42-G, Computer Security for Nuclear Security, 2021, p. 16. Available at: https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1918_web.pdf.

IIoT can provide benefits to the nuclear energy sector across many vectors, including safety, cyber security, and efficient operations.

Benefits of IIoT Deployment in Nuclear Facilities

This section identifies use cases for nuclear power plants to leverage IIoT. Considerations such as the business case, safety impact, and security risks will determine whether such use cases are reasonable to implement.

Condition Monitoring, Predictive Maintenance, Age Management

Operation and maintenance are typically the main cost drivers in a nuclear power plant, representing between 40 and 70 percent of overall generating costs.[27] Downtime, meaning time not producing electricity, additionally costs 1 to 2 million USD daily. Avoiding unplanned equipment repairs and optimising maintenance policies can provide significant cost savings. IIoT enables real-time monitoring of critical equipment such as turbines, pumps, and cooling systems. By analysing sensor data (e.g. vibration, temperature, pressure) and plant performance data, online condition monitoring and predictive maintenance analysis can detect early signs of wear or failure. This reduces unplanned downtime, extends equipment life, and minimises the risk of catastrophic failures.

Enhanced Safety Monitoring and Emergency Management

Nuclear safety is paramount for NPP operations. While NPP safety and plant operational systems are isolated networks, key safety parameters may be transmitted offsite to an Emergency Management Site and/or the regulator.

27 Leonord J. Bond et al., "Improved Economics of Nuclear Plant Life Management", IAEA-CN-155-008KS, In Proceedings of Second International Symposium on Nuclear Power Plant Life Management, Shanghai, 15–18 Oct 2007. Available at: https://www-pub.iaea.org/MTCD/Publications/PDF/P1362_CD/htm/pdf/Keynote%20Speakers/008KS.pdf.

In the United States this is implemented through the Emergency Response Data System, which involves the direct electronic transmission of selected parameters from the NPP.[28] IIoT supports the expansion of this capability and the use of advanced analytical capabilities, as noted in the example under the digital twin section below.

Plant Operations Efficiency

IIoT provides granular visibility and situational awareness of integrated plant operations and external factors, enabling decision support and resource optimisation. Real-time data analytics help plant management fine-tune systems for maximum efficiency and plan for and mitigate the impact of both internal and external disruptions, promoting plant reliability and resilience.

Cyber Security Integration

Just as IIoT enables real-time monitoring of physical attributes of critical equipment, it can also support the collection of computer network traffic and endpoint cyber parameters. This data can then be sent to an on-site or external security operations centre (SOC) for monitoring and analysis to detect anomalies and signs of cyber compromise. This is a common use case of IIoT in nuclear facilities.

Digital Twin Implementation

A digital twin (DT) is the virtual representation of an object or system designed to reflect a physical object accurately.[29] A key attribute of a DT is real-time data. This data is typically integrated with an AI engine to produce a realistic view of a nuclear facility and project future states. For safety-adjacent applications, DT models must undergo rigorous verification and validation to ensure that outputs are accurate, explainable, and do not introduce risks when used for operational or regulatory decision support. For example, a DT intended to model reactor coolant system behaviour should first be validated against historical transient data (e.g. startup, shutdown, or load-following events) to demonstrate that its predictions remain within the bounds of known plant performance. The implementation of a DT for a nuclear facility would offer significant benefits for both operators (i.e. licensees) and regulators. DT technology could provide a shared platform for real-time situational awareness, thereby enhancing safety margins and regulatory efficiencies.[30] Studies have also examined the use of DT technologies to support condition monitoring[31] and cyber security.[32]

Inventory and Supply Chain Management

IIoT could assist in managing the flow of consumables and spare part inventories across multiple suppliers and distribution chains. IIoT enables real-time visibility and control over supply chain assets, improving efficiency, reducing waste, and enhancing responsiveness. IIoT could integrate active tracking of parts/commodities, both internal and external to the organisation, to support inbound logistics monitoring and warehouse inventory optimisation. IIoT solutions might also include controls for end-to-end traceability to address concerns related to counterfeit, fraudulent, and suspect items and parts. Additionally, IIoT could assess natural and man-made hazards that could impact required inventories and supplies.

28 Bezakulu Alemu, “Emergency Response Data System”, US Nuclear Regulatory Commission, NUREG-1394, Rev. 2, Aug 2022, p. 2-1. Available at: https://www.nrc.gov/docs/ML2224/ML22244A081.pdf.

29 Nick Gallagher and Maggie Mai Armstrong, “What is a digital twin?”, IBM, 12 Apr 2020, updated Oct 2025. Available at: https://www.ibm.com/topics/what-is-a-digital-twin.

30 Neal R. Gross and Co., Inc, Official Transcripts of the Proceedings, Nuclear Regulatory Commission, “Advisory Committee on Reactor Safeguards”, 4 May 2022, p. 96. Available at: https://www.nrc.gov/docs/ML2217/ML22179A369.pdf.

31 Diaa-Eldin Mansour et al., “Applications of IoT and digital twin in electrical power systems: A comprehensive survey”, IET Generation, Transmission & Distribution, Vol. 17, Issue 20, Oct 2023, p. 4468.

32 David Allison, Paul Smith, and Kieran McLaughlin, “Digital Twin Architecture for Cybersecurity Incident Response in Instrumentation and Control Systems”, presented at the Nuclear Plant Instrumentation and Control & Human-Machine Interface Technology (NPIC&HMIT 2025), American Nuclear Society, Jun 2025, pp. 534–543. Available at: https://www.ans.org/pubs/proceedings/article-58901/.

Remote Monitoring and Control

Monitoring and controlling distributed assets are a potentially strong use case for IIoT implementation. The operating and security paradigm in a Gen III NPP, however, does not support remote control for critical functions, such as those supporting nuclear safety and nuclear security, as remote operation was not part of the plant's design or safety analysis. Remote monitoring and control, however, may be a consideration and design feature of advanced reactors whose concepts include the capability for remote and autonomous operations.[33]

33 Shannon Eggers and Robert Anderson, "Cyber-Informed Engineering for Nuclear Reactor Digital Instrumentation and Control", in Nuclear Reactors – Spacecraft Propulsion, Research Reactors, and Reactor Analysis Topics, ed. by Chad L. Pope, 29 March 2022, p. 7. Available at: https://doi.org/10.5772/intechopen.101807.

Data and cyber security risks are some of the chief concerns connected to the implementation of IIoT in the nuclear sector.

Challenges and Risks of IIoT in Nuclear Facilities

The implementation of IIoT at an NPP is not without costs, challenges, and risks. Some organisations may determine that these factors outweigh the potential benefit of IIoT and the potential associated shift in the operational paradigm. Decisions to forgo an IIoT solution can stem from a variety of strategic, financial, operational, and cultural reasons. A discussion of the most common challenges is set out in the following sections.

Unclear Business Case and Costs

NPP designs and operational processes have been developed under strict performance and regulatory requirements, and design modifications and process changes may be required for IIoT system integration. However, the business case offered by proposed IIoT integration may not be sufficient to warrant such changes. The associated return on investment may be uncertain or take too long to realise, and leadership may struggle to justify the cost without clear, measurable benefits.

IIoT implementation, likewise, requires significant investment in hardware, software, the work of integration (e.g. establishing processes), training, and change management. Smaller or budget-constrained organisations may find this cost to be financially prohibitive, especially when a strong business case may not exist.

Legacy Systems and Infrastructure Integration

Recall the example of the automobile and phone from the introduction. Now try to remember the state of phone and car technology five, 10, and 15 years ago. The differences in capability are significant. Today's phones and cars are substantially more advanced. It is not uncommon, however, to see a 20-year-old car driving down the road. Why, with significant achievements in technology, has the car owner not upgraded to the newest model? The reasons given by the owner could be that the car still functions as needed, the cost of replacement is too much, maintenance and operation are known and easy, and the old car provides a sense of familiarity and trust. Their attitude could be one of "fix it when it breaks, drive it till it stops". The same rationale applies to many legacy systems in an NPP, which becomes problematic for IIoT integration.

This philosophy, however, becomes somewhat problematic given that many computers and digital components may have an End of Life (EOL) of 3 to 8 years.[34] As an example, the date 14 October 2025 marks the product End of Support (EOS) for Microsoft Windows 10. After this point, Microsoft will no longer provide free security updates, technical assistance, or feature updates for Windows 10.[35] Organisations are encouraged to migrate to Windows 11. A review of digital systems at an NPP would likely find in use Windows 10, Windows 7 (EOL: 14 Jan 2020[36]), Windows XP (EOL: 8 Apr 2014[37]), and many even older OS versions as well as other EOL application software. Software updates are also likely not planned. Similarly, one can examine the associated computer hardware and find components beyond the end of the Original Equipment Manufacturer (OEM) support. DCS are designed for a 15 to 20-year life cycle.

While current computer systems and industrial products are designed to support and embrace IIoT integration,[38,39] legacy software and hardware may not meet the connectivity and data collection requirements for IIoT solutions. The legacy equipment challenges may even affect newly commissioned NPPs.

Retrofit and modernisation of digital infrastructure may alleviate these challenges, but digital transformation is extremely expensive in terms of engineering and downtime costs. Digital system updates or even augmentation may likewise not be possible due to "simple" logistics and engineering factors, such as:[40]

- Lack of server cabinet space or other physical space
- Inadequate heat dissipation for additional computer equipment
- Lack of cable runs or communication conduits for information transmission
- Lack of a power source
- Exceeding physical load limitations

The limitations of legacy systems and the reluctance or inability to update such systems makes IIoT integration a challenge for existing reactor and plant designs. Note that this situation will be different for new designs and new builds, therefore anticipating and planning for IIoT should be a design function in the development of Gen IV and advanced reactors. These new builds will have an advantage in fully realising the benefits of IIoT.

34 HP, "What's the Average Computer Lifespan? A Guide for U.S. Users", HP Tech Takes, 24 Sep 2024. Available at: https://www.hp.com/us-en/shop/tech-takes/average-computer-lifespan#:~:text=Remember%2C%20while%20the%20average%20lifespan,%2C%20maintenance%2C%20and%20specific%20needs.

35 Microsoft Corporation, "End of support for Windows 10, Windows 8.1, and Windows 7", accessed Oct 2025. Available at: https://www.microsoft.com/en-us/windows/end-of-support?r=1.

36 Microsoft Corporation, "Windows 7", accessed Oct 2025. Available at: https://learn.microsoft.com/en-us/lifecycle/products/windows-7.

37 Microsoft Corporation, "Windows XP", accessed Oct 2025. Available at: https://learn.microsoft.com/en-us/lifecycle/products/windows-xp.

38 AVEVA, "The Industrial Internet of Things (IIoT) Solutions", accessed Oct 2025. Available at: https://www.aveva.com/en/solutions/digital-transformation/industrial-internet-of-things/?_gl=1*ywtul5*_up*MQ..*_gs*MQ..&gclid=EAIaIQobChMIjKOJzZnBjgMVo5uDBx0iHSMZEAAYASAAEgLTw_D_BwE.

39 Siemens, "SIMATIC IOT gateways", Siemens Products and Services, accessed Oct 2025. Available at: https://www.siemens.com/global/en/products/automation/industrial-computing/iot-gateways.html.

40 Faisal Mousa, Ibrahim Al Bousi, and Doanld Dudenhoeffer, "Operating Experience in Implementing Cyber Security in a New Build NPP", in Proceedings of the 2023 IAEA International Conference on Computer Security in the Nuclear World: Security for Safety, 2023.

Data and Cyber Security Concerns

The application of effective and sufficient security measures to IIoT systems poses unique security challenges, which include, but are not limited to:

- **Diverse Device Landscape:** Thousands of sensors, actuators, and controllers – many with limited computing power or outdated firmware – make standardised security difficult.
- **Legacy Systems:** Many industrial systems were not originally designed with consideration for cyber security.
- **Limited Visibility:** Traditional IT monitoring tools struggle to inspect and manage operation technology (OT) environments.
- **High Availability Requirements:** Downtime in industrial systems can lead to significant financial and safety consequences.

The best security model for IIoT frameworks is not a single framework but a multi-layered, defence-in-depth approach that applies security measures at all layers of IIoT interaction. A significant body of standards and literature has been developed to guide the secure implementation of IIoT, which includes, but is not limited to:

- **IEC 62443:** Focuses on industrial control systems security
- **National Institute of Standards and Technology IoT Security Framework:** Offers comprehensive guidelines for securing IoT systems
- **International Organization for Standardization (ISO)/IEC 27001:** Establishes an Information Security Management System
- **Open Worldwide Application Security Project IoT Top 10:** Highlights common vulnerabilities and mitigation strategies
- **Industrial Internet Consortium (IIC) Industrial Internet Security Framework:** Tailored for IIoT environments

Data Security

The IIoT framework is highly reliant on data flows that often extend beyond one organisation's premises. The networks used for communication may be dedicated networks, but more likely they are commercial networks. Likewise, cloud infrastructure is commonly used to support data storage and/or processing. Data security and data sovereignty are in this context, significant concerns.[41]

Organisational data used in IIoT applications is often sensitive and proprietary to that organisation. Unauthorised access to or disclosure of this information could have significant adverse financial and security consequences. The benefit of an IIoT framework is its ability to integrate multiple data streams to produce actionable results. However, within this data consolidation (data fusion), organisations are often concerned with maintaining the confidentiality, integrity, and sovereignty of their own data.

A federated data space is an example of a data management strategy to overcome these challenges. A federated data space is a decentralised framework that enables secure and controlled data sharing across multiple organisations or entities, without requiring the data to be stored in a central repository. Instead of aggregating data in one place, users retain control over their data access and usage. Gaia-X, a European initiative, is an example of a federated data space.[42]

41 States may have data sovereignty laws related to critical infrastructure that require data from such organisations to reside within the physical boundaries of the State. This can become problematic given the cross-border reach of IIoT frameworks and cloud infrastructure.

42 Gaia-X European Association for Data and Cloud AISBL," What is Gaia-X", accessed Oct 2025. Available at: https://gaia-x.eu/what-is-gaia-x/.

Zero Trust Architecture

Zero Trust Architecture (ZTA) has emerged as a compelling security model for use in IIoT environments. Zero Trust is a security paradigm built on the principle of "never trust, always verify".[43] Rather than assuming trust based on network location or device identity, Zero Trust demands continuous authentication and strict access control for every user, device, and application – regardless of whether they are inside or outside the network. The application of ZTA has been evaluated for use within nuclear facilities and with the following proposed Zero Trust principles:[44]

- **Assume Hostile Environment:** This applies to both inside and outside the NPP and implies that initially all users, devices, and networks are untrusted.
- **Presume Breach:** Assume breach has already occurred in your network.
- **Never Trust, Always Verify:** Access is denied by default, each device, user, request is authenticated, and authorisation granted based on least privilege and dynamic policies.
- **Scrutinise Explicitly:** Requests, actions, and behaviour are continuously monitored.
- **Security Maintains Safety:** The security decisions and enforcement of the decisions must not affect the safety-related and important-to-safety functions of the facility.

The National Institute for Standards and Technology further defines the basic tenets for ZTA implementation:[45]

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy – including the observable state of client identity, application/service, and the requesting asset – and may include other behavioural and environmental attributes.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorisation are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture.

Are such tenets achievable at an NPP? Sandia National Laboratories conducted research evaluating ZTA principles applicable to nuclear power control systems. Their conclusion was that tenets (3), (4), and (6) were essentially impossible to implement in current nuclear power plant control systems, as their implementation could increase latency and introduce new failure vectors.[46]

Security is likewise not without costs. The implementation of ZTA can introduce significant complexity. Moreover, IIoT frameworks, by their very nature, already introduce additional layers of connectivity and data flows. Such complexity may conflict with nuclear I&C system safety design guidance, which emphasises minimising "unnecessary complexity" and "[keeping] the I&C system as simple as possible" to maintain safe and reliable operational functions.[47]

43 ACT-IAC, "Zero Trust Cybersecurity Current Trends," American Council for Technology-Industry Advisory Council (ACT-IAC), 18 Apr 2019. Available at: https://www.actiac.org/zero-trust-cybersecurity-current-trends.

44 Anya Kim and Kim Lawson-Jenkins, , "Implementing Zero Trust for Operational Technology at Nuclear Facilities," Technical Letter Report TLR-RES-DE-2025-001, U.S. Nuclear Regulatory Commission, Feb 2025, p. 1. Available at: https://www.nrc.gov/docs/ML2504/ML25041A017.pdf.

45 Scott Rose et al., " Zero Trust Architecture," NIST Special Publication 800-207, U.S. Department of Commerce, Aug 2020, pp. 6-7. Available at: https://csrc.nist.gov/pubs/sp/800/207/final.

46 Benjamin Karch et al., "Zero Trust Architectures in Nuclear Control Systems", Sandia National Laboratories, Sandia Report, 2024, p. 6. Available at: https://www.sandia.gov/app/uploads/sites/273/2024/11/ZTA_Report.pdf.

47 International Atomic Energy Agency, "Design of Instrumentation and Control Systems for Nuclear Power Plants", IAEA Safety Standards Series, No. SSG-39,2016, p. 50. Available at: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1694_web.pdf.

Regulatory Uncertainty

Nuclear power is one of the most regulated industrial sectors, and with good reason, as a safety or security event could have global consequences. The general regulatory approach to new technology integration is cautious and technology neutral. Examples of regulatory approaches to new technologies can be seen in a joint report on AI integration in nuclear applications issued by the Canadian Nuclear Safety Commission (CNSC), United Kingdom's Office for Nuclear Regulation (UKONR), and the USNRC, as well as in the UKONR's own evaluation, which explicitly states the current "goal-setting, outcome focused, risk-based regulatory framework is technology neutral".[48,49]

The key to regulatory acceptance of new technology integration in nuclear facilities relates to the specific function that technology performs and the associated potential risk to nuclear safety (and nuclear security) that would occur in the case of a system failure or maloperation (such as by a malicious act).[50] As the complexity of systems increase, likewise does the challenge of explainability and provability of deterministic results required for regulatory assurance. This scrutiny further increases as the level of autonomy increases, alongside the potential adverse impact on nuclear safety and security functions. This does not preclude the use of IIoT but may limit near-term applicability to passive functions not linked directly to system control.

Staffing and Lack of Internal Expertise

As with many new technologies, IIoT requires specialised skills in networking, data analytics, cyber security, and systems integration. Organisations may lack the talent or resources to manage the transition, operation, and maintenance of the IIoT solution, requiring either outsourcing, internal staff development, or a combination of both.

IIoT system integration may also impact the workforce at multiple levels. An example of this is the integration of AI into organisations, which has the potential to dramatically alter current job functions and associate workforce knowledge, skills, and abilities requirements. Likewise, the use of IIoT can be a paradigm shift from current proximal operations requiring change management to build workforce acceptance and promote the effective use of the newly introduced technology and associated processes.

Operational Disruption

NPPs are designed for 24/7 operation and electricity generation. Non-production periods are costly, minimised, and tightly managed. Organisations may be averse to the time requirements and impact on operations that implementing an IIoT solution might take. Likewise, since implementing an IIoT solution may increase system complexity and reliance on internal infrastructure, recovery from impactful events may be more challenging and lengthier. An example of this is the September 2025 cyberattack on Jaguar Land Rover (JLR) in the United Kingdom. The attack brought to a halt three JLR UK smart manufacturing facilities responsible for production of 1,000 cars daily.[51] Production at JLR UK facilities was shutdown for over a month and led to £485m loss over the same period last year and an additional cost of £196m for cyber related expenses associated with recovery from the attack.[52]

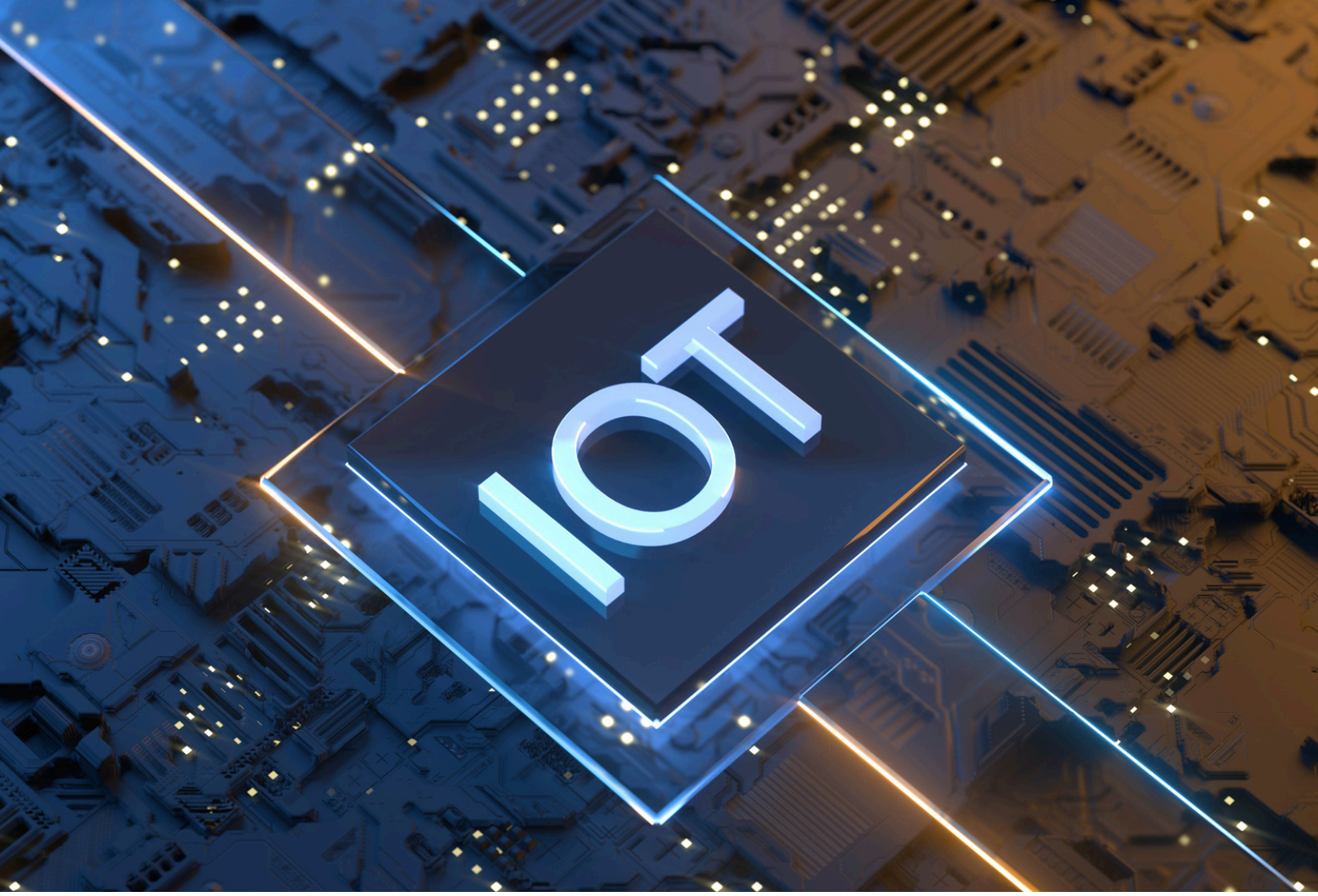
48 UKONR, "ONR's pro-innovation approach to AI regulation", ONR Policy, Issue 1, Apr 2024, p. 5. Available at: https://www.onr.org.uk/media/v45dkpu2/onr-pro-innovation-approach-to-ai-regulation-paper.pdf.

49 CNSC, UKONR, and USNRC "Considerations for Developing Artificial Intelligence Systems in Nuclear Applications", Sep 2024. Available at: https://onr.org.uk/media/03zl1osf/canukus_trilateral_ai_principles_paper_2024_08_28-final.pdf.

50 Donald Dudenhoeffer, "Past, Present, and Future Applications of AI in the Nuclear Sector", Vienna Center for Disarmament and Non-Proliferation (VCDNP), Apr 2025, p. 45. 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.

51 Jack Fitzgerald, "After a Cyberattack Brought JLR to a Halt, Production is Restarting", Car and Driver, updated 30 Sep 2025. Available at: https://www.caranddriver.com/news/a66125275/jlr-cyberattack-timeline/.

52 Theo Leggett, "Jaguar Land Rover posts heavy loss after cyber-attack", BBC News, 14 November 2025. Available at: https://www.bbc.com/news/articles/ckg1w255gy1o.



IIoT offers tremendous opportunities for both the current fleet of NPPs and future advanced reactors.

Conclusion

IIoT represents more than just a framework – it introduces a transformative work paradigm that enables high-speed data exchange between edge devices and physical assets, or "things". It integrates capabilities such as remote monitoring, performance analytics, and seamless connectivity with diverse, distributed applications to support functions like inventory control, workflow optimisation, and strategic planning. IIoT offers the potential for real-time analysis, insights, and interaction between connected and potential distal objects.

IIoT offers tremendous opportunities for both the current fleet of NPPs and future advanced reactors. NPPs have traditionally existed as isolated production environments to support safety and security concerns. IIoT stretches this mindset to include workflows that integrate distributed and highly communicative objects and processes.

However, the implementation of IIoT in an NPP is not trivial and requires a level of system integration and network infrastructure to support data collection and exchange. Challenges frequently exist regarding updating current Gen III NPP operational systems to support digital transformation, such as that required for IIoT. Challenges include, among others, the cost-benefit justification for the particular use case, managing integration with legacy plant systems, and cyber security risk management. Instances of IIoT solutions do exist in current NPPs, and the ongoing digital transformation at nuclear facilities, coupled with the push to adopt emerging technologies like AI, will accelerate the adoption of IIoT solutions. Yet, the real promise for IIoT will be in the design and development of advanced reactors. Planning for and leveraging IIoT capabilities and requirements early in the design process will provide for more effective and secure implementations.

The successful deployment of IIoT in a nuclear power plant environment requires a measured and methodical approach that integrates business objectives, technical feasibility, regulatory expectations, and operational safety. A pragmatic roadmap for IIoT adoption in nuclear facilities can be summarised in five steps:

1. **Inventory Data of Value:** Identify critical assets and prioritise data sources that provide measurable operational, safety, or economic benefits.

2. **Safe Egress Pattern:** Establish secure, regulator-approved pathways for data transfer, such as brokered historians or unidirectional gateways.

3. **Pilot Use Cases (Non-Safety Systems):** Begin with low-risk applications (e.g. inventory management, environmental monitoring) to build confidence and quantify value.

4. **Governance and Model Risk for AI:** Define governance structures, regulatory compliance processes, and validation frameworks for AI/ML models embedded in IIoT workflows.

5. **Scale with Zero Trust Architecture Controls:** Expand deployment to additional use cases under a defence-in-depth model, applying ZTA principles, as applicable, to ensure security and resilience.

This structured progression provides nuclear operators with a pathway to realise IIoT benefits while maintaining the sector's paramount commitment to safety and security.

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