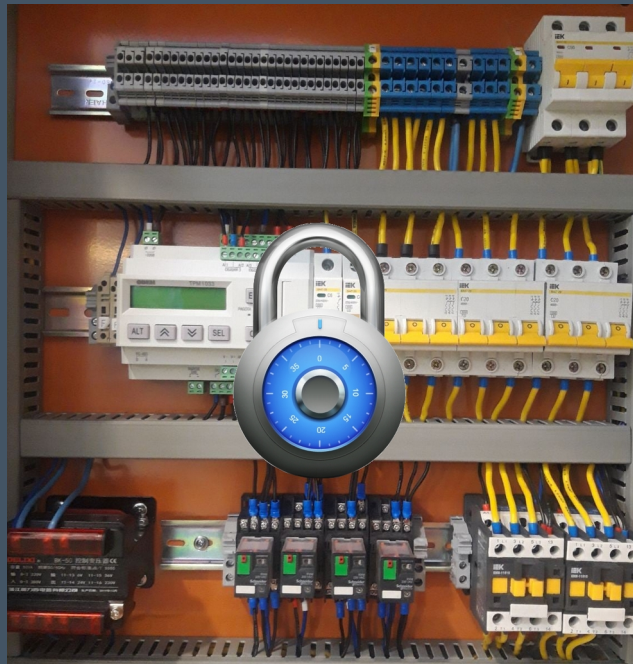


Topic 1

Industrial Environments & the Purdue Architecture



Dr Diarmuid Ó Briain
Version: 1.0

Copyright © 2026 C²S Consulting

Licensed under the EUPL, Version 1.2 or – as soon they will be approved by the European Commission - subsequent versions of the EUPL (the "Licence");

You may not use this work except in compliance with the Licence.

You may obtain a copy of the Licence at:

https://joinup.ec.europa.eu/sites/default/files/custom-page/attachment/eupl_v1.2_en.pdf

Unless required by applicable law or agreed to in writing, software distributed under the Licence is distributed on an "AS IS" basis, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the Licence for the specific language governing permissions and limitations under the Licence.

Dr Diarmuid Ó Briain



Table of Contents

1 Objectives.....	4
2 Introduction.....	4
3 Introduction & High-Level Comparison.....	5
3.1 Information Technology.....	5
3.2 Operational Technology.....	5
3.3 Consideration of Security Implications.....	6
4 The Core OT Philosophy.....	7
4.1 Industrial Security: Inverting the CIA Triad.....	7
4.2 Safety, Availability, Integrity, Confidentiality for OT.....	8
5 The Structural Network Blueprint.....	10
5.1 Purdue Enterprise Reference Architecture.....	10
5.2 PERA Levels.....	10
5.3 IT/OT Architecture.....	12
5.4 Firewalls.....	13
5.5 Differences between IT and OT.....	13
6 Historical Impact Context.....	15
7 Bibliography.....	16

Illustration Index

Figure 1: OT -v- IACS -v- ICS.....	6
Figure 2: Inverting the CIA Triad.....	7
Figure 3: Brewery.....	9
Figure 4: Purdue Enterprise Reference Architecture.....	10
Figure 5: PERA Layer Descriptions.....	11
Figure 6: OT Architecture.....	12
Figure 7: OT/ICS Cybersecurity Incidents Over Time.....	15

Index of Tables

Table 1: Comparison between SCADA and DCS.....	6
Table 2: Differences between IT and OT.....	13

1 Objectives

By the end of this topic, you will be able to:

- Contrast Information Technology (IT) with Operational Technology (OT) across functional, operational, and lifecycle dimensions.
- Analyse the unique security implications that arise when legacy, deterministic industrial systems intersect with modern enterprise networks.
- Explain the standard Confidentiality, Integrity, Availability (CIA) Triad and justify the critical requirement to invert it into an Availability-Safety-Integrity-Confidentiality framework for OT Security (OTSec).
- Deconstruct the Purdue Enterprise Reference Architecture (PERA) model, identifying the core functions, network boundaries, and security enforcement points (firewalls) for Levels 0 through 5.
- Evaluate historical OT cybersecurity incidents to identify how structural or architectural failures allowed real-world cyber physical compromises.

2 Introduction

For decades, IT and OT existed in completely separate silos. IT professionals focused on data, web connectivity, enterprise applications, and the corporate network, operating under the assumption that systems could be regularly patched, rebooted, and upgraded. Meanwhile, plant engineers managed physical real-world events, controlling pumps, adjusting valves, regulating electrical grids, and maintaining assembly lines. These OT systems were designed for deterministic behaviour, human safety, and absolute uptime, frequently operating on isolated legacy protocols with expected lifecycles measured in decades.

Today, those silos have collapsed. The drive for business intelligence, predictive maintenance, and remote efficiency has forced the convergence of IT and OT.

This topic session explores the architecture born from that convergence. It will examine why traditional IT security mindsets fail, and can even cause physical harm, when blindly applied to an active industrial plant. By dissecting the structural blueprints of the PERA and mapping how data must securely cross from the corporate boardroom down to the factory floor, the topic will focus the foundational engineering principles required to defend modern critical infrastructure.

3 Introduction & High-Level Comparison

3.1 Information Technology

Any equipment or interconnected system used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an organisation or by a 3rd party on the organisations behalf.

IT includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

3.2 Operational Technology

Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include Industrial, Automation and Control Systems, Building Management Systems (BMS), Fire Control Systems (FCS), and Physical Access Control mechanisms.

The landscape of OT is vast and varied, requiring cybersecurity practitioners to develop a nuanced understanding of different environments to apply the correct security concepts and risk assessments. In heavy industrial sectors, such as power generation, facilities are often classified as Critical National Infrastructure (CNI). These sites are characterised by their massive physical scale and the grave implications for public stability and human life should a failure occur. In these high-stakes settings, the primary challenge lies in balancing traditional IT security perspectives with the absolute necessity of maintaining operational safety and continuous uptime.

In contrast, manufacturing environments for specialised goods, such as advanced medical hardware, present a different set of complexities. While these facilities may have a smaller physical footprint than a power utility, they often manage highly sensitive intellectual property and stringent quality control standards. Across all these sectors, a defining characteristic is the presence of hybrid architectures. Modern facilities rarely run on a single unified platform; instead, they utilise a mixture of Supervisory Control And Data Acquisition (SCADA) systems for broad monitoring and Distributed Control Systems (DCS) for precise, real-time process management. Integrating ageing legacy components with modern automated systems remains one of the most significant hurdles in securing the modern industrial enterprise.

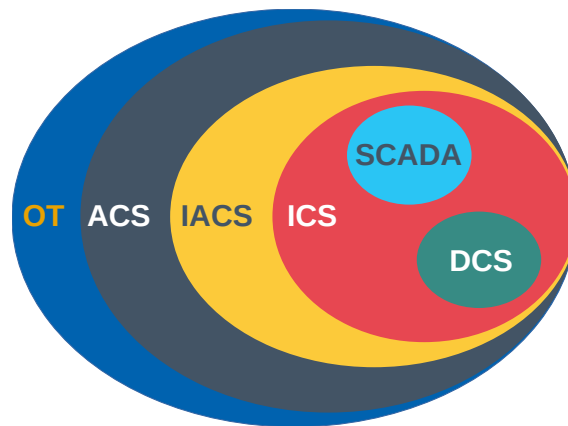


Figure 1: OT -v- IACS -v- ICS

3.2.1 SCADA and DCS

To better understand the functional differences between these two foundational technologies, it is helpful to compare how they manage data and control across an industrial environment. While both systems are essential to modern operations, they are designed with distinct priorities: SCADA focuses on high-level oversight and wide-area data collection, whereas a DCS is engineered for intensive, high-speed process management within a specific facility. Table 1 highlights the key technical and architectural differences that cybersecurity practitioners must account for when securing these assets.

Table 1: Comparison between SCADA and DCS

Feature	SCADA	DCS
Focus	Data acquisition and remote monitoring	Process control and system integration
Location	Geographically dispersed (pipelines, power grids)	Centrally located (refineries, chemical plants)
Control Logic	Event-driven (waits for a change)	Process-driven (continuous loops)
Reliability	Good, but dependent on communication links	Extremely high (redundancy is built-in)
Data Handling	Collects data from many remote sites	Manages a massive stream of local data

3.3 Consideration of Security Implications

Consider the security implications of having a network that has legacy systems, such as Windows XP, connected to it. It is not just workstations and server systems to consider but also old network infrastructures such as switches, routers and firewalls.

4 The Core OT Philosophy

4.1 Industrial Security: Inverting the CIA Triad

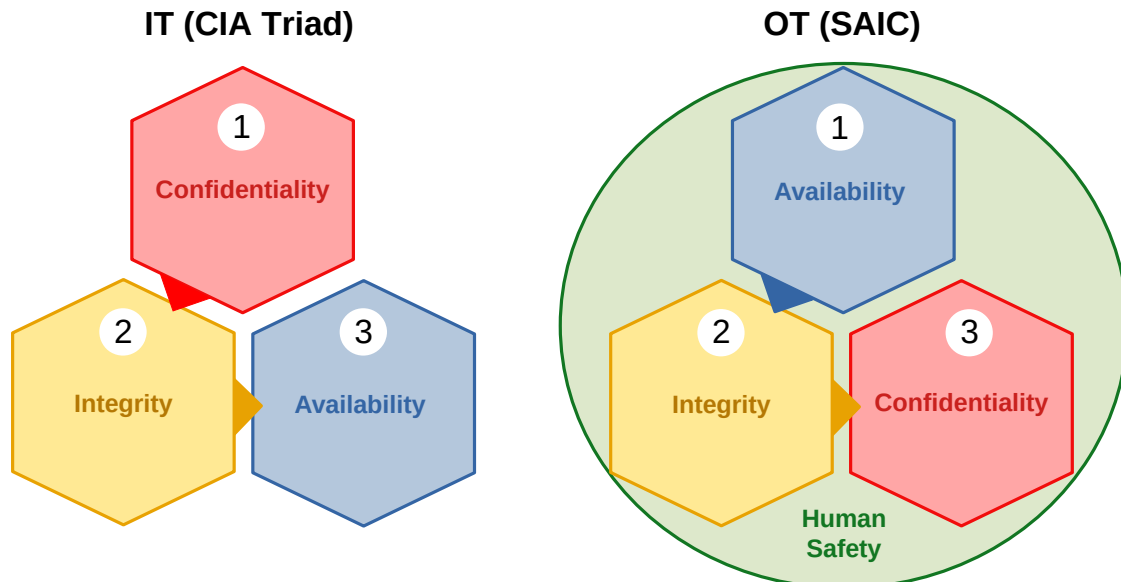


Figure 2: Inverting the CIA Triad

For many years, information security has held Confidentiality, Integrity and Availability (known as the CIA triad) as the core principles of information security.

4.1.1 Confidentiality

Confidentiality is the term used to prevent the disclosure of information to unauthorised individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorised party obtains the card number in any way, a breach of confidentiality has occurred.

Breaches of confidentiality take many forms. Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality. If a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in a breach of confidentiality. Giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorised to have the information.

Confidentiality is necessary (but not sufficient) for maintaining the privacy of the people whose personal information a system holds.

4.1.2 Integrity

In information security, integrity means that data cannot be modified without authorisation. This is not the same thing as referential integrity in databases. Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorised user vandalises a web site, when someone is able to cast a very large number of votes in an online poll, and so on.

There are many ways in which integrity could be violated without malicious intent. In the simplest case, a user on a system could miss-type someone's address. On a larger scale, if an automated process is not written and tested correctly, bulk updates to a database could alter data in an incorrect way, leaving the integrity of the data compromised. Information security professionals are tasked with finding ways to implement controls that prevent errors of integrity.

4.1.3 Availability

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.

4.2 Safety, Availability, Integrity, Confidentiality for OT

Security was not initially considered as an important factor when designing an ICS. In fact, often, it was not considered because of the fear that implementing security controls could reduce the availability of the system. For example, in a case where a power station is continually producing power, then any stoppage has a big impact to the process. Stopping and starting a complete power station process can take significant time, so undertaking a patch that involves restarting a critical device may have to wait for days, weeks or even months before a patch window might be given.

Therefore the IT core principals of the CIA triad, with confidentiality being the most important, is completely inverted when OT systems are considered. First and foremost is Human Safety, then the Availability of the system, closely followed by Integrity, are far more important than Confidentiality in this case, the Safety, Availability, Integrity, Confidentiality (SAIC).

4.2.1 Example



Figure 3: Brewery

A brewery's main Production Management Software (PMS), actually running outside of the Industrial Automation and Control Systems (IACS), in the enterprise network, was affected by malware. Because the production management system was down, the production line had to be halted. Because the production line was stopped, no product is coming off the line that could be packed and shipped. The resulting logjam, then also means that goods coming in can not be unloaded, and production line employees are unable to do their jobs.

This is why Availability is more important than Confidentiality in OT.

Data however is still very important within OT as proprietary knowledge and confidential product information can all be stored and transmitted as part of a OT network.

In the brewery, the recipes and process timings have to be stored, and security controls, by necessity, have to be focused on keeping production running, but also on protecting companies intellectual property that are also likely to be on the network.

5 The Structural Network Blueprint

5.1 Purdue Enterprise Reference Architecture

The PERA, or Purdue Model, is a foundational framework for modelling and integrating enterprise-wide systems, particularly in the context of Operational [1].

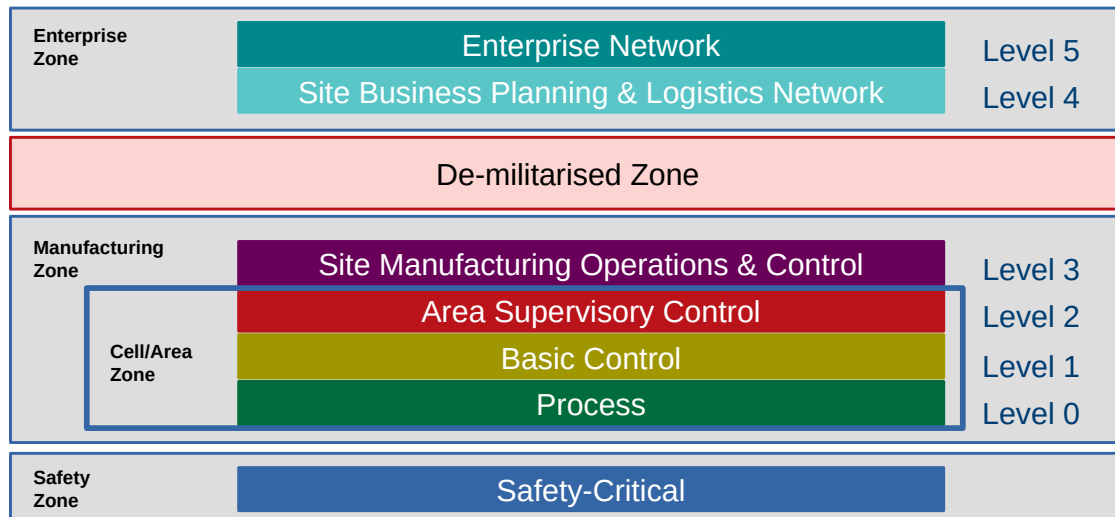


Figure 4: Purdue Enterprise Reference Architecture

PERA, as illustrated in Figure 4, has a well known hierarchical structure, or layered model, which provides a clear and distinct separation between OT and IT as well as between the various functional levels within an organisation with an OT environment.

The model was developed in the 1990s at Purdue University for Computer-Integrated Manufacturing (CIM) to map data flows and define best practices for the relationship between control systems and business networks.

It has been widely adopted as a conceptual guide for OT security, defining where controls should be placed and how communication should flow between different layers.

5.2 PERA Levels

As detailed in Figure 5, the architecture divides the network into distinct levels, typically including a De-Militarised Zone (DMZ) for controlled communication. This layered approach is fundamental to the model's design, establishing a hierarchy of control and information flow from the physical process up to the business systems. The DMZ (Level 3.5) acts as a crucial buffer or secure gateway between the high-security OT network (Levels 0-3) and the less-trusted, broader IT network (Levels 4-5). This separation is vital for network segmentation, ensuring that even if the business network is compromised, the critical industrial processes remain isolated and protected.

Level	Zone	Function	Example Systems
5	Enterprise Network	Corporate business logistics and management.	Enterprise Resource Planning (ERP), corporate email, databases.
4	Site Business Planning and Logistics Network	Managing business-related activities of the manufacturing operation.	Manufacturing schedules, material use, inventory.
3.5	DMZ	A buffer or convergence layer between the IT and OT networks.	Jump servers, firewalls, data historians, patch management.
3	Site Manufacturing Operations & Control	Managing production work flow to produce desired products.	Manufacturing Execution Systems (MES), batch management.
2	Area Supervisory Control	Supervising, monitoring, and controlling the physical processes.	SCADA, Human-Machine Interface (HMI).
1	Basic Control	Sensing and manipulating the physical processes.	Programmable Logic Controllers (PLC), Remote Terminal Units (RTU).
0	Physical Process	The actual physical equipment.	Sensors, actuators, pumps, motors.

Figure 5: PERA Layer Descriptions

5.3 IT/OT Architecture

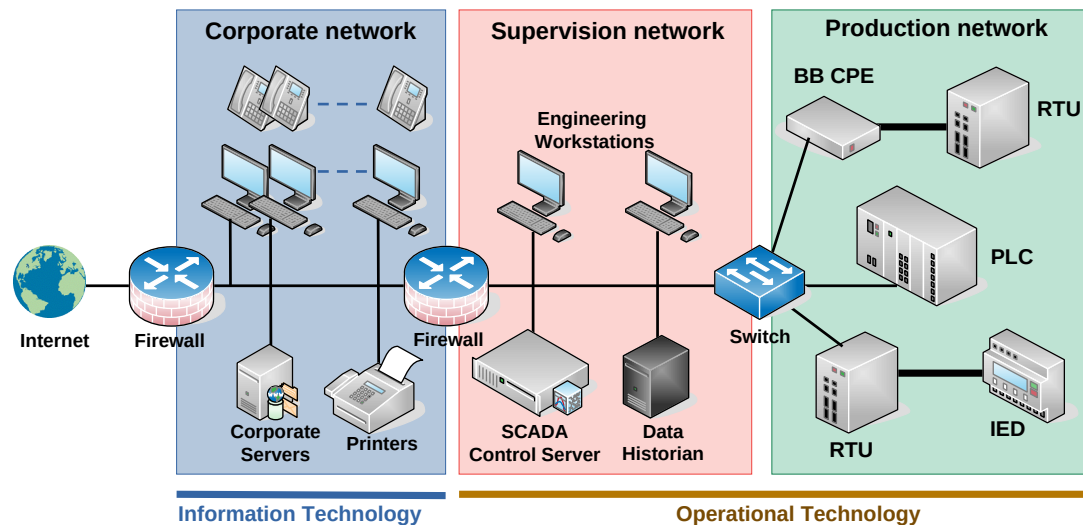


Figure 6: OT Architecture

Consider the OT generic architecture illustrated in Figure 6.

5.3.1 Production network

On the right side there is the production network, also known as the in-process network. Within this network there are RTUs and Intelligent Electronic Devices (IED), wired and wireless industrial networks, PLCs and HMIs connected to those PLCs. All of these devices connect to physical devices. For example, alarm systems, actuators and valves to name a few. Here are physical devices that have real impacts to operations, most importantly safety.

5.3.2 Supervision network

This network consists of either DCS, SCADA, or a combination of both. In the diagram a SCADA network displayed that consists of supervision controls where operators manage system operations, maintenance laptops that provide more technical teams to make changes or adjustments, and data historians. The data historians collect the production network data for devices that can then send this data to corporate networks.

5.3.3 Corporate network

The corporate network may need to interact with the Supervision network. For example, key metrics that may help the organisation understand when a device is reaching its end of life and allow for planning to implement a replacement. Within corporate networks there are common corporate IT networks, Enterprise Resource Planning (ERP) and production management servers that are common across most corporate organisations. These corporate networks connect to the Internet to perform all the common business functions for an organisation.

Most cyber security training today is IT-focused. There is a learning curve for OT and their operations as they are not necessarily IT. There are very different environments. SCADA environments with PLC networks, serial communications, so there is a

difference and an understanding is necessary not only the technical components of OT world, but an understanding of the philosophy and the different mindset and the methodologies around it. A combination of the two is required.

5.4 Firewalls

While there is obviously a requirement for a firewall between the organisation and the Internet there is also a requirement for a firewall to secure the supervisory and production networks from the corporate network. This is critical to prevent the corporate network being used as a conduit to the OT.

5.4.1 Data Diode

In cases where that level of security between the networks is particularly critical an organisation may choose to employ a Data diode. These are used to segment and defend networks, and transfer information in one direction only. They allow data to be sent from a secured network/segment, such as the supervisory network, to external systems and users such as the corporate network, cloud based services, a remote monitoring facility or regulatory bodies while limiting the attack vector back into the secured network.

5.5 Differences between IT and OT

The following lists some special considerations when considering security for OT [2]:

Table 2: Differences between IT and OT

Category	IT	OT
Performance Requirements	• Non-real time. • Response must be consistent. • High throughput is demanded. • High delay and jitter may be acceptable. • Emergency interaction is less critical. • Tightly restricted access control can be implemented to the degree necessary for security.	• Real-time. • Response is time-critical. • Modest throughput is acceptable. • High delay and/or jitter is not acceptable. • Response to human and other emergency interaction is critical. • Access to OT should be strictly controlled but should not hamper or interfere with human-machine interaction.
Availability (Reliability) Requirements	• Responses such as rebooting are acceptable. • Availability deficiencies can often be tolerated, depending on the system's operational requirements.	• Responses such as rebooting may not be acceptable because of process availability requirements. • Availability requirements may necessitate redundant systems. • Outages must be planned and scheduled days/weeks in advance. • High availability requires exhaustive pre- deployment testing.

Category	IT	OT
Risk management requirements	• Manage data. • Data confidentiality and integrity is paramount. • Fault tolerance is less important – momentary downtime is not a major risk. • Major risk impact is delay of business operations.	• Control physical world. • Human safety is paramount, followed by protection of the process. • Fault tolerance is essential; even momentary downtime may not be acceptable. • Major risk impacts are regulatory non-compliance, environmental impacts, and loss of life, equipment, or production.
System operation	• Systems are designed for use with typical OSs. • Upgrades are straightforward with the availability of automated deployment tools.	• Systems often use differing and possibly proprietary OSs, sometimes without security capabilities built in. Software changes must be carefully made, usually by software vendors, because of the specialised control algorithms and perhaps modified hardware and software involved.
Resource constraints	• Systems are specified with enough resources to support the addition of third-party applications such as security solutions.	• Systems are designed to support the intended industrial process and may not have enough memory and computing resources to support the addition of security capabilities.
Communications	• Standard communications protocols. • Primarily wired networks with some localised wireless capabilities. • Typical IT networking practices.	• Many proprietary and standard communication protocols. Several types of communications media used, including dedicated wire and wireless (radio and satellite). Complex networks that sometimes require the expertise of control engineers.
Change management	• Software changes are applied in a timely fashion in the presence of good security policy and procedures. The procedures are often automated.	• Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of the OT system is maintained. OT outages often must be planned and scheduled days/weeks in advance. OT may use OSs that are no longer supported.
Managed support	• Allow for diversified support styles.	• Service support is usually via a single vendor.
Component lifetime	• Lifetime on the order of three to five years.	• Lifetime on the order of 10 to 15 years.
Components location	• Components are usually local and easy to access.	• Components can be isolated, remote, and require extensive physical effort to gain access to them.

6 Historical Impact Context

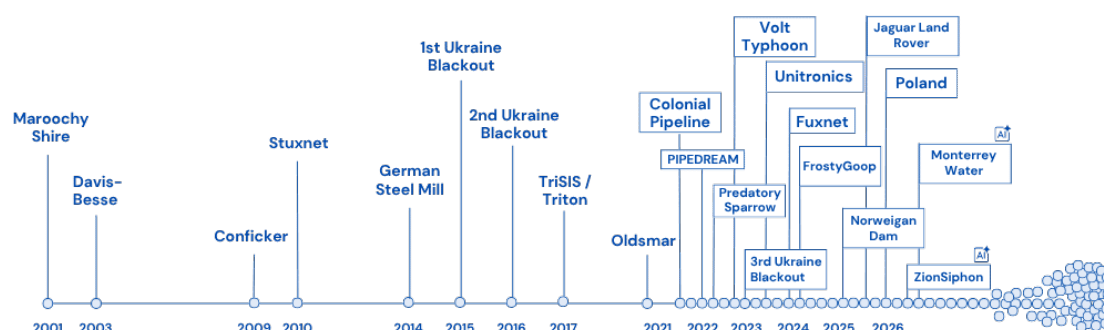


Figure 7: OT/ICS Cybersecurity Incidents Over Time

Figure 7 illustrates a historical timeline of major cybersecurity incidents, specifically targeting OT and critical infrastructure from 2001 through 2026. It traces the evolution of industrial cyber threats, beginning with early landmark events such as the Maroochy Shire sewage breach in 2001 and the discovery of Stuxnet in 2010, before showing a massive surge in both the frequency and complexity of attacks in recent years. By mapping out notorious incidents, such as the Ukrainian power grid blackouts, the Colonial Pipeline ransomware attack, and emerging threats such as Volt Typhoon, the figure underscores a dramatic shift from isolated, sporadic disruptions to an increasingly crowded and volatile modern threat landscape.

7 Bibliography

- [1] T. J. Williams, 'The Purdue enterprise reference architecture', *Computers in industry*, vol. 24, no. 2–3, pp. 141–158, 1994.
- [2] K. Stouffer *et al.*, *NIST SP 800-82r3 Guide to Operational Technology (OT) Security*, Standard NIST SP 800-82 Rev. 3, Sep. 28, 2023. Accessed: Oct. 30, 2023. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf>