

Industrial Environments & the Purdue Architecture

Dr Diarmuid Ó Briain

9 Sep 2026



Licence



This work is licenced under a Creative Commons
Attribution-ShareAlike 4.0 International Licence.
Full Licence: <http://creativecommons.org/licenses/by-sa/4.0>

Module sections

- **Theme 1: OT Infrastructure & Foundational Security**
 - Pre-Reading: Foundations, History & Taxonomy
 - Topic 1: Industrial Environments & the Purdue Architecture
 - Topic 2: Hardening OT Components & Physical Boundaries
 - Topic 3: Layered Logical Access Control & Core Protocols
 - TBL 1: Design a secure entry and access policy for a critical manufacturing facility



Module sections

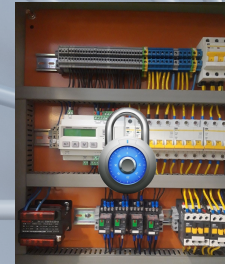
- **Theme 2: Governance, Risk, and Compliance (GRC)**
 - Pre-Reading: Strategic GRC Foundations & Taxonomy
 - Topic 4: Enterprise Risk Management Frameworks & Threat Quantification
 - Topic 5: Strategic Governance & Operational Security Frameworks
 - Topic 6: ISMS Architecture, Regulatory Audits & Forensic Readiness
 - TBL 2: Auditing a company against a framework and conducting a high-level risk assessment.



Module sections

- **Theme 3: Offensive Security & Incident Response**

- Pre-Reading: Threat Fundamentals & Environment Setup
- Topic 7: Proactive Defence & Offensive Reconnaissance
- Topic 8: Incident Response & Breach Management (Immersive Simulation)
- TBL 3: The Recce-to-Response Crisis.



Industrial Environments & the Purdue Architecture

Dr Diarmuid Ó Briain

9 Sep 2026

setu.ie
INSPIRING FUTURES



Version: 1.0

Learning objectives

- At the end of this topic you will be able to:

- Contrast IT with 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 CIA Triad and justify the critical requirement to invert it into an Availability-Safety-Integrity-Confidentiality framework for OT Security.
- Deconstruct the 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.

Exercise



OT in use

- Consider a holiday flight you have taken, enjoyable? Yes. Now go back and consider the OT devices you interacted with, but in your excitement you probably didn't notice.
- In pairs discuss and list some:



OT in use

Which of the following industrial locations use OT devices?

- A) Airport
- B) Dam
- C) Salmon farm
- D) Cake factory
- E) Power station
- F) Train station
- G) Pharmaceutical plant
- H) Creamery
- I) All of the above

OT in use

Which of the following industrial locations use OT devices?

- A) Airport
- B) Dam
- C) Salmon farm
- D) Cake factory
- E) Power station
- F) Train station
- G) Pharmaceutical plant
- H) Creamery
- I) **All of the above** ✓

SE TU
Ollscoil
Teicneolaíochta
an Oirdheiscirt
South East
Technological
University

Introduction & High-Level Comparison

INSPIRING FUTURES

Topic introduction

- The Collapse of Traditional Silos: IT/OT.
- Drivers of IT/OT Convergence.
- The Risk of Blindly Applying IT Security to OT.
- Architectural Blueprint for Defence, dissecting PERA to ensure data securely crosses from the boardroom to the factory floor.

IT versus OT

• Information Technology (IT)

- 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.

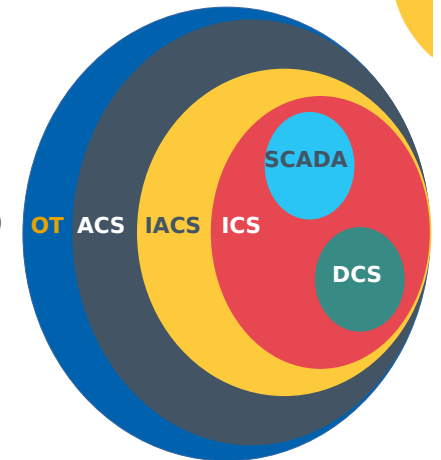
IT versus OT

• Operational Technology (OT)

- 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:
 - Automation and Control Systems (ACS)
 - Building Management Systems (BMS)
 - Fire Control Systems (FCS)
 - Physical Access Control Systems (PACS).

Some OT Terms

- Operational Technology (OT)
- Automation and Control Systems (ACS)
- Industrial Automation and Control Systems (IACS)
- Industrial Control Systems (ICS)
- Supervisory Control and Data Acquisition (SCADA)
- Distributed Control System (DCS)



SCADA -v- 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

Exercise

The Power Station



Operational Technology (OT)

- What is different about this power station and a typical office environment in terms of computing?

ESB Aghada,
Cork, Ireland

Operational Technology (OT)

- What is different about this power station and a typical office environment in terms of computing?
 - Computing interacts with physical processes.
 - There is the potential for physical damage.
 - There is a real risk to human life.
 - Wider implications for society if the station is disrupted.

ESB Aghada,
Cork, Ireland

Operational Technology (OT)

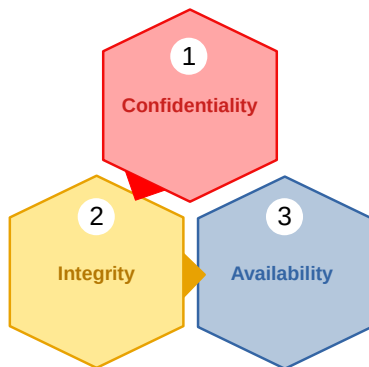
- Securing and managing large-scale critical infrastructure requires prioritising human safety and operational uptime over traditional IT data-security practices:
 - The size of such facilities and the concerns for operations and security.
 - Balancing the IT perspective and the OT perspective.
 - The paramount importance of safety concerns for health and human life.

ESB Aghada,
Cork, Ireland

The Core Operational Technology (OT) Philosophy

Core principles of information security

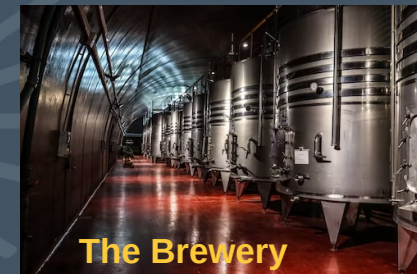
IT (CIA Triad)



OT (SAIC)



Exercise



The Brewery

Example

- A brewery's main Production Management Software (PMS), actually running outside of the ACS, in the enterprise network, was affected by malware.

What are the implications?

Example

- A brewery's main Production Management Software (PMS), actually running outside of the ACS, in the enterprise network, was affected by malware.
 - Because the PMS 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.

What does this demonstrate?

Example

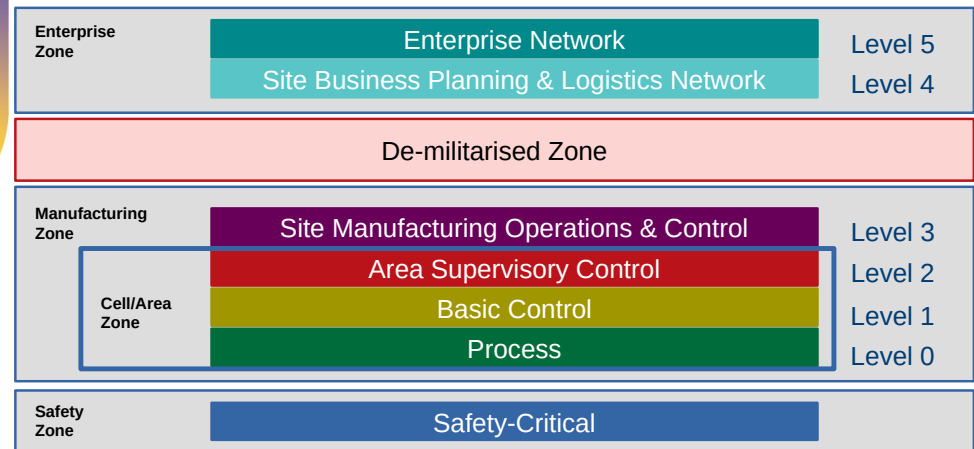
- This is why **Availability** is more important than **Confidentiality** in OT.
- Data is still very important within OT as proprietary knowledge and confidential product information can all be stored and transmitted as part of a OT network.
 - In a brewery, the recipes and process timings have to be 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.

The Structural Network Blueprint

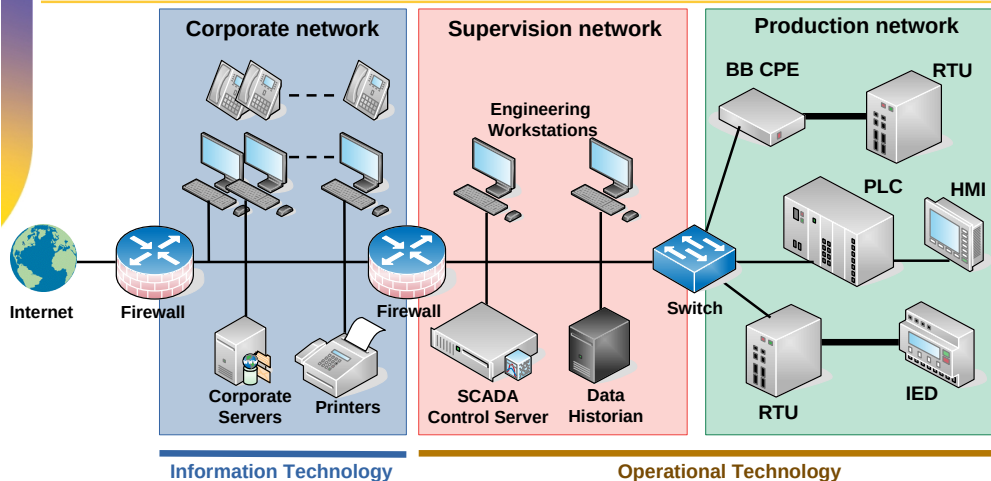
Purdue Enterprise Reference Architecture (PERA)

- A hierarchical, layered model for integrating enterprise-wide systems, especially in OT environments.
- It provides a clear and distinct separation between the OT and IT domains.
- The structure defines different functional levels within an organisation, guiding the placement of systems and controls.
- Developed in the 1990s for Computer-Integrated Manufacturing (CIM) to map data flows between control systems and business networks.
- Widely adopted as a conceptual guide for OT security, defining communication flow and control placement between layers.

Purdue Enterprise Reference Architecture (PERA)



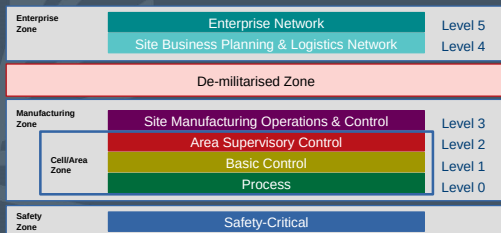
SCADA Architecture



Categories of differences between IT/OT

- Performance Requirements
- Availability Requirements
- Risk management requirements
- System operation
- Resource constraints
- Communications
- Change management
- Managed support
- Component lifetime
- Components location

Exercise



PERA

What is wrong with PERA

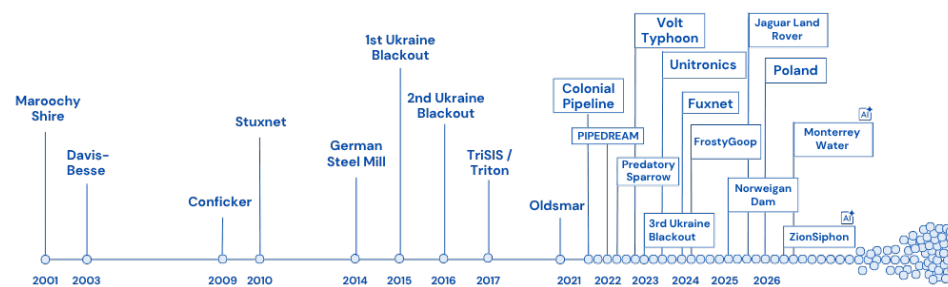
- Consider PERA as described and identify the weakness in the architecture?
- How would you solve it?



**Electrical Interconnector
converter station
Ballyadam, Cork**

Historical Impact Context

OT/IACS Cybersecurity Incidents Over Time



Exercise



Quiz



Facility Footprint

Why is the size of an electricity generation plant relevant?

- A) The larger the footprint, the more networking connectivity required, hence more Assets to monitor and protect
- B) The larger the footprint, the greater use of Wi-Fi networking
- C) The larger the footprint, the more physical security controls that are required
- D) All of the above

Facility Footprint

Why is the size of an electricity generation plant relevant?

- A) The larger the footprint, the more networking connectivity required, hence more Assets to monitor and protect
- B) The larger the footprint, the greater use of Wi-Fi networking
- C) The larger the footprint, the more physical security controls that are required
- D) **All of the above** ✓

Securing Legacy Systems

Consider an electricity power generation plant with legacy control systems with Windows XP monitoring /control stations. They cannot be upgraded or touched in any way. What is the most optimal method for securing these assets?

- A) Place these assets on an isolated VLAN network
- B) Create a zone that is specific to the operational requirement and then restrict connectivity between zones
- C) Add Anti-virus software to workstations
- D) Upgrade to the latest version of Windows OS

Securing Legacy Systems

Consider an electricity power generation plant with legacy control systems with Windows XP monitoring /control stations. They cannot be upgraded or touched in any way. What is the most optimal method for securing these assets?

- A) Place these assets on an isolated VLAN network
- B) **Create a zone that is specific to the operational requirement and then restrict connectivity between zones** ✓
- C) Add Anti-virus software to workstations
- D) Upgrade to the latest version of Windows OS

OT Vulnerabilities

Which of these is a TOP vulnerability impacting OT cybersecurity?

- A) The use of Unmanaged Desktops and Laptops
- B) The use of vulnerable Software
- C) Monitoring of OT Systems
- D) Cybersecurity training

OT Vulnerabilities

Which of these is a TOP vulnerability impacting OT cybersecurity?

- A) The use of Unmanaged Desktops and Laptops
- B) **The use of vulnerable Software** ✓
- C) Monitoring of OT Systems
- D) Cybersecurity training

Managing Risk in IT and OT

As an IT Security or IT Operations person coming into an IACS Cybersecurity environment, what is your primary goal?

- A) Protect Assets and Reduce Risk
- B) Protect Revenue while maintaining Operational Availability
- C) Measure the risks and Control them, then see where you can improve your process
- D) Find the potential risks, measure those risks, set acceptable limits for the risk, review and re-examine those limits, then repeat
- E) Find the potential risks, then control them, then assess them, after that you can relax a bit
- F) Control risk at all times and in all situations, then measure it, then review that measurement and then find possible risks

Managing Risk in IT and OT

As an IT Security or IT Operations person coming into an IACS Cybersecurity environment, what is your primary goal?

- A) **Protect Assets and Reduce Risk** ✓ [3]
- B) **Protect Revenue while maintaining Operational Availability** ✓ [2]
- C) Measure the risks and Control them, then see where you can improve your process
- D) **Find the potential risks, measure those risks, set acceptable limits for the risk, review and re-examine those limits, then repeat** ✓ [1]
- E) Find the potential risks, then control them, then assess them, after that you can relax a bit
- F) Control risk at all times and in all situations, then measure it, then review that measurement and then find possible risks



Learning Outcomes

SE TU Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

INSPIRING FUTURES

setu.ie | 46

Learning outcomes

You should now be able to:

- Contrast IT with 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 CIA Triad and justify the critical requirement to invert it into an Availability-Safety-Integrity-Confidentiality framework for OT Security. ✓
- Deconstruct the 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. ✓



SE TU Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

EUR ING Dr Diarmuid Ó Briain
Innealtóir Cairte agus Léachtóir Sinsearach

D +353 59 917 5000 | E diarmuid.obriain@setu.ie | setu.ie
Campas Bhóthar Chill Chainnigh, Ceatharlach, R93 V960, Éire

Thank you

engcore
advancing technology

INSPIRING FUTURES

setu.ie | 48