

Hardening OT Components & Physical Boundaries

Dr Diarmuid Ó Briain

16 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>

Learning objectives

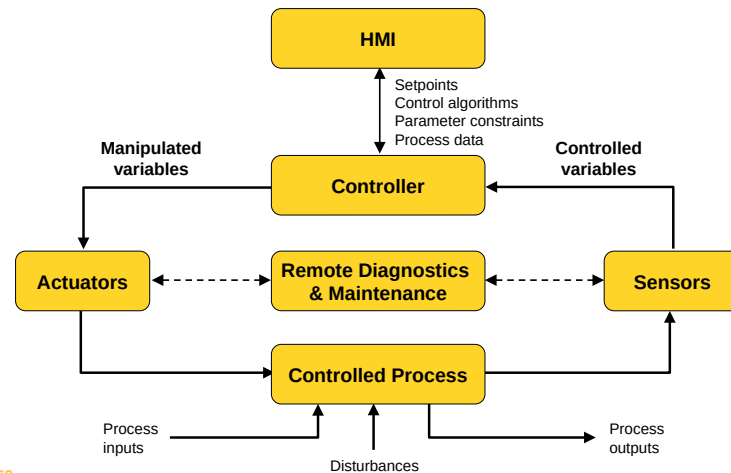
- At the end of this topic you will be able to:
 - Deconstruct the industrial hardware stack, explaining the relationship between transducers, control loops, fieldbuses, and PLCs.
 - Compare and Contrast the operational roles, scales, and architectural boundaries of SCADA, DCS, and SIS.
 - Evaluate physical security perimeters, site designs, and environmental mitigation controls (HVAC, fire, power) designed to protect critical assets.
 - Justify why physical access control is fundamentally linked to digital integrity in an operational technology environment.

The OT Hardware Stack

Typical OT Systems

- OT systems consist of combinations of control components that act together to achieve an **objective**.
- The part of the system primarily concerned with producing an output is referred to as the **process**.
- The part of the system primarily concerned with maintaining conformance with specifications is referred to as the **controller**.
- The system can be configured in one of three ways:
 - Open-loop**: the output is controlled by established settings
 - Closed-loop**: the output has an effect on the input in such a way as to maintain the desired control objective
 - Manual mode**: the system is controlled completely by human input.

Typical OT System



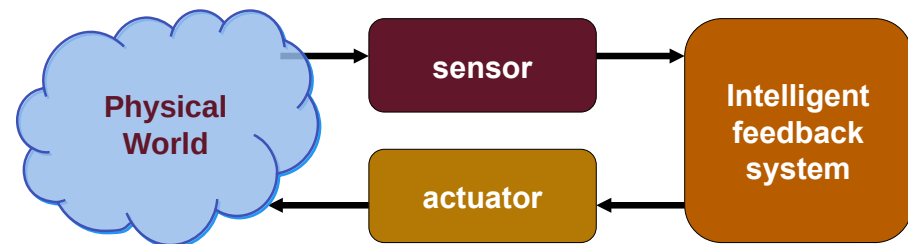
Control loops

The factors that heavily influence the design of OT systems can also help determine the system's security needs.

Such factors are:

- Control Timing Requirements
- Geographic Distribution
- Hierarchy
- Control Complexity
- Availability
- Impact of Failures
- Safety.

Transducers



Sensors

A sensor is a transducer that converts a physical stimulus from one form into a more useful form to measure the stimulus

- Two basic categories:
 - Analogue - 4 – 20 mA signal representation
 - Discrete
 - Binary – boolean output (i.e. reed, proximity and photoelectric)
 - Digital – sensor converts to digital (i.e. temperature, Ph level, pressure)



Sound
(db pressure)



Touch



Light
(light intensity)



Ultrasonic
(distance)

Actuators

- Electrical actuators
 - Electric motors
 - DC servomotors
 - AC motors
 - Stepper motors
 - Solenoids
- Hydraulic actuators
 - Use hydraulic fluid to amplify the controller command signal
- Pneumatic actuators
 - Use compressed air as the driving force



Programmable Logic Controller (PLC)

- A device with a programmable memory for:
 - internal storage of instructions
 - the implementation of specific functions, such as logic, sequencing, timing, counting and arithmetic.
- To control through analogue or digital input/output modules various types of machines or process.



PLC control

Which of the following is NOT an example of something connected to a PLC?

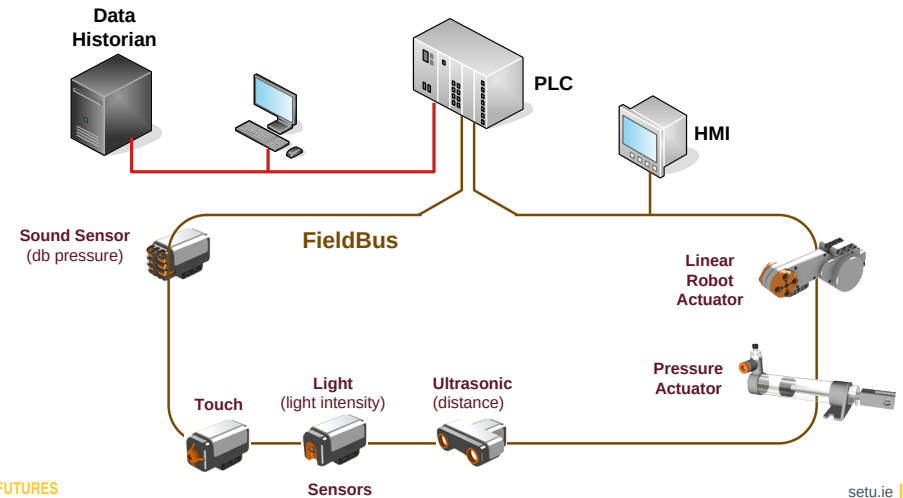
- A) Temperature sensor
- B) Robot arm actuator
- C) Pressure valve
- D) Fire hose
- E) None of the above

PLC control

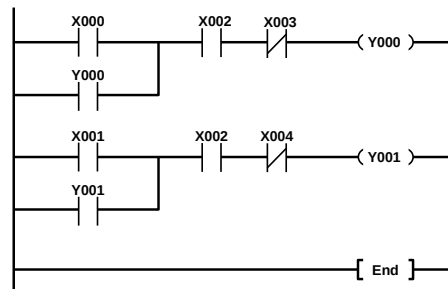
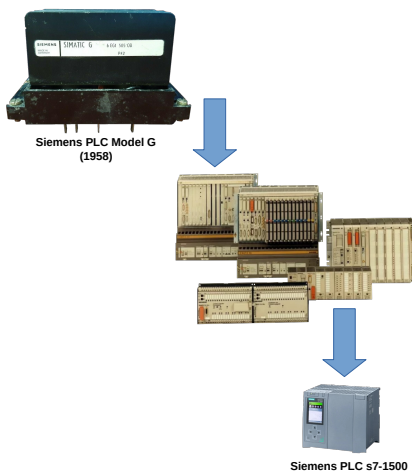
Which of the following is NOT an example of something connected to a PLC?

- A) Temperature sensor
- B) Robot arm actuator
- C) Pressure valve
- D) Fire hose ✓
- E) None of the above

PLC Control System



Ladder Logic



Fieldbus

Which of the following are considered a Fieldbus?

- A) RS232 connections from the PLC to the sensors and actuators carrying 4 – 20 mA signals?
- B) A non-time-critical communications system, such as Ethernet
- C) A deterministic Ethernet like network such as Time Sensitive Networking (TSN)
- D) None of the above

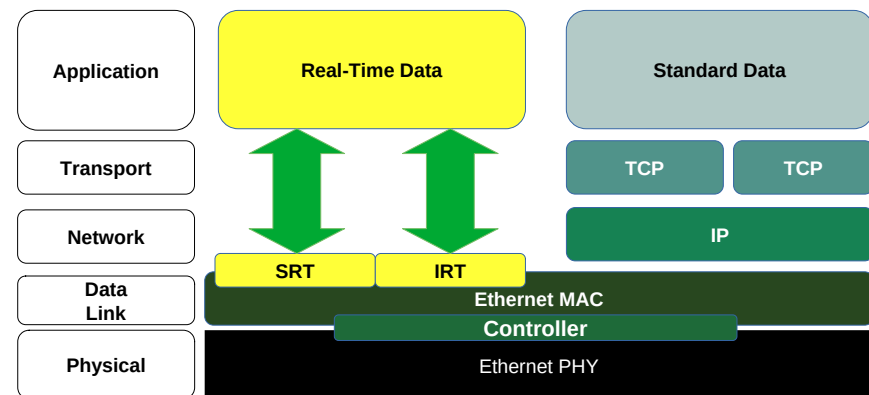
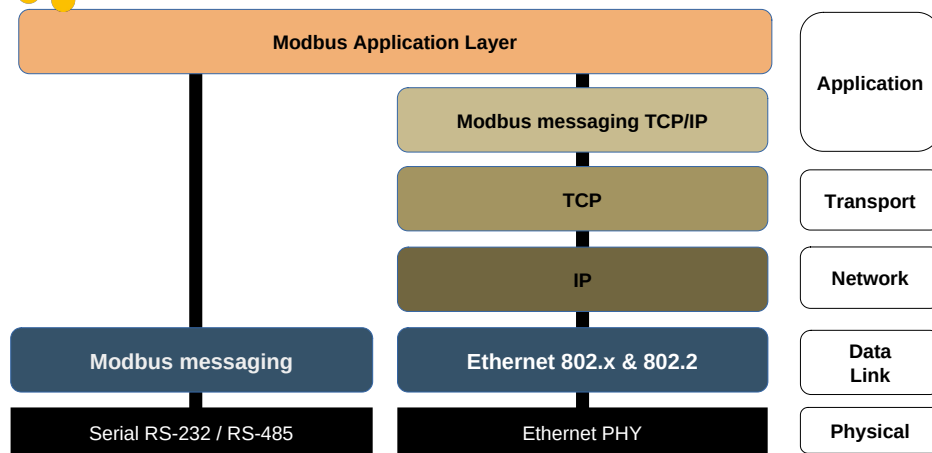
Fieldbus

Which of the following are considered a Fieldbus?

- A) RS232 connections from the PLC to the sensors and actuators carrying 4 – 20 mA signals?
- B) A non-time-critical communications system, such as Ethernet
- C) **A deterministic Ethernet like network such as TSN** ✓
- D) None of the above

Fieldbus Protocols and standards

- **Modbus and Modbus TCP/IP**
 - Master-slave application-layer protocol.
- **Distributed Network Protocol version 3 (DNP3)**
 - A set of open communication protocols.
 - IEEE recommendation for RTU to IED messages.
 - No in-built security, messages can be intercepted, modified and fabricated.
- **IEC 60870-5 suite:**
 - Substation control centre communication.
 - Communication with protection equipment.
 - Security implementation.



Fieldbus Protocols and standards

- **Process Field Network (ProfiNet)**

- Master-slave application-layer protocol
- Time constraint friendly
- Fast data exchange between Ethernet-based field devices
- ProfiNet Soft-Real Time (SRT) – Frames are directed from Layer 2, directly to the ProfiNet Layer 7, skipping the TCP/IP layers - thus improving the speed and determinism.
 - The end performance overall depends on the network design but cycle times 512ms down to 250µs are possible to achieve.
- ProfiNET Isochronous Real-Time (IRT) goes a step beyond the SRT, eliminating the variable data delays (jitter) in high network traffic by enhancing the rules for the Ethernet traffic and creating special rules for ProfiNet traffic.
 - Fulfills all synchronisation requirements allowing a deterministic communication with 31.25µs and 1µs of jitter.

INSPIRING FUTURES

setu.ie | 21

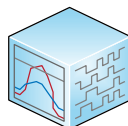
Industrial Systems Scaling

INSPIRING FUTURES

setu.ie | 22

Supervisory Control and Data Acquisition (SCADA)

- SCADA is an important part of OT
- SCADA was originally designed for communication challenges with phone lines, microwaves, satellites
- SCADA is a *centralised* computerised system that is capable of gathering and processing data and applying operational controls over long distances as a collection of both software and hardware.



INSPIRING FUTURES

setu.ie | 23

Exercise



INSPIRING FUTURES

setu.ie | 24

Scenario: ESB NT and fallen tree on line

- A tree falls on a line and locals report that sparks are coming from the area and a heavy duty wire is jumping around.
- **Before SCADA**
 - Engineer needed go to a nearby fuse/link on the line, at a nearby location to make sure disconnect the spur to make the situation safe.
 - How long until the line was made safe?

Scenario: ESB NT and fallen tree on line

- A tree falls on a line and locals report that sparks are coming from the area and a heavy duty wire is jumping around.
- **Before SCADA**
 - Engineer needed go to a nearby fuse/link on the line, at a nearby location to make sure disconnect the spur to make the situation safe.
 - How long until the line was made safe?
- **With SCADA**
 - SCADA immediately trips the breaker at the feeding sub-station
 - When an engineer can get to the site, they will disconnect a smaller spur section to the specific problem and inform the SCADA operator to reenergise the remainder of the line to return power to the remaining customers.

SCADA risks

- What risks do you see with the introduction of SCADA in this example?



SCADA and vulnerabilities

Which of these technological changes are increasing cybersecurity vulnerability for SCADA systems?

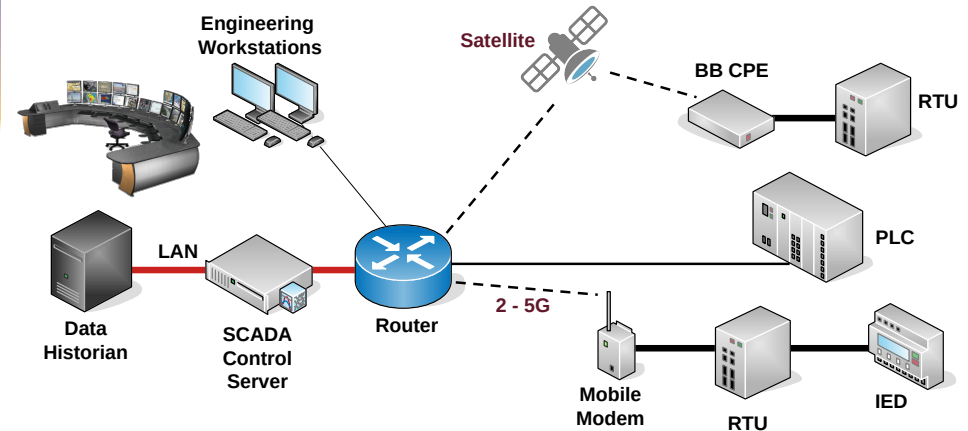
- A) Flashing lights on train station signalling control boards
- B) Advancements in IoT
- C) Ethernet & Internet connectivity
- D) Physical control switches

SCADA and vulnerabilities

Which of these technological changes are increasing cybersecurity vulnerability for SCADA systems?

- A) Flashing lights on train station signalling control boards
- B) **Advancements in IoT** ✓
- C) **Ethernet & Internet connectivity** ✓
- D) Physical control switches

OT Architecture



Remote Terminal Units (RTU)

- Transmit telemetry data to the master system, and respond to messages from the master supervisory system to control connected objects



Intelligent Electronic Device (IED)

- Microprocessor-based controllers of power system equipment, such as circuit breakers, transformers and capacitor banks.



Distributed Control Systems (DCS)

- While SCADA is centralised, DCS are a *decentralised* system that distributes control functions among multiple controllers located close to the process equipment.
- DCS systems typically use *closed-loop control*, where control parameters are automatically adjusted based on feedback from sensors.
- Individual DCS controllers are located in the same geographical location of an industrial site, so a factory or a power plant, communicates with different control elements within a single factory.

Safety Instrumented Systems (SIS)

- Another OT system to take into account is SIS.
- These are dormant systems, or passive systems, and they do not respond until they are called into action.
- They can be found in most industrial environments.
- **Example:** a pressure release valve
 - When the pressure is increased there needs to be some type of a safety system in order to release that pressure when limits are exceeded, which could result in an explosion.
 - Such SIS must be considered in terms of security because the risk to life, or they create another attack vector.

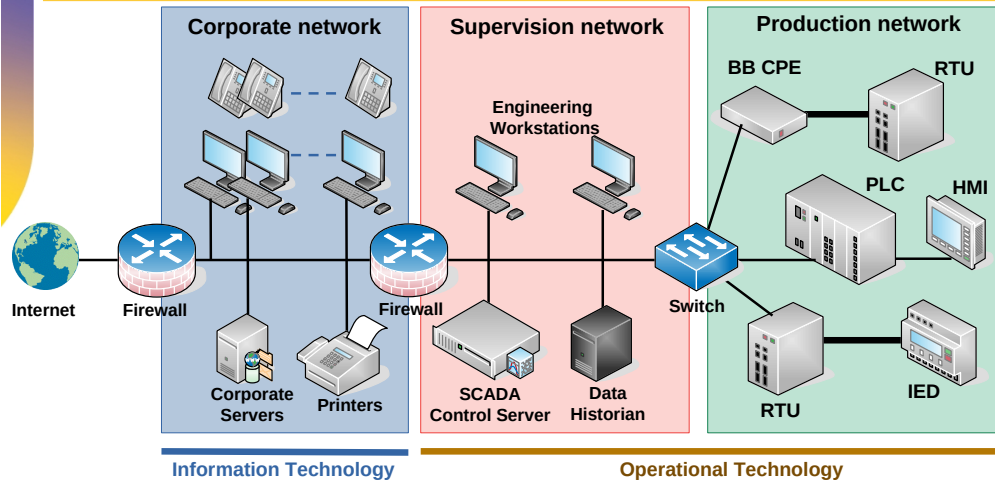


Fire suppression system

Comparison of SCADA/DCS/SIS

Feature	SCADA	DCS	SIS
Primary Goal	Monitor and control large, dispersed systems.	Automate and optimise a single, localised process.	Ensure process safety and prevent catastrophic failure.
Geographic Scope	Very large areas (e.g., pipelines, grids).	Single plant or facility.	Subsystem within a plant.
Control Style	Supervisory; operator-driven.	Automated, continuous, closed-loop.	Independent, automated, fail-safe.
Control Logic	Event-driven	State-driven	Event-driven
Communication	Wide area, varied networks.	High-speed local network.	Dedicated, isolated, and redundant.
Key Risk	Wide attack surface; remote access vulnerabilities.	Centralised control compromise.	Failure to respond in an emergency.
Example Use	Power grid, water distribution.	Chemical plant, refinery.	Emergency Shutdown System (ESD).

SCADA Architecture



INSPIRING FUTURES

setu.ie | 37

Physical Site Perimeter Defences

INSPIRING FUTURES

setu.ie | 38

Layered Physical Access Control Systems (PACS)

*How secure do
you consider
this barrier?*

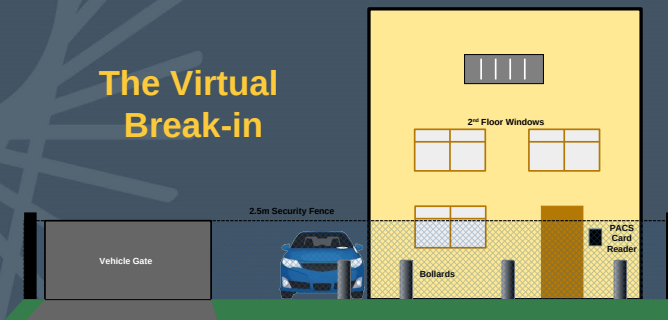


INSPIRING FUTURES

setu.ie | 39

Exercise

The Virtual Break-in



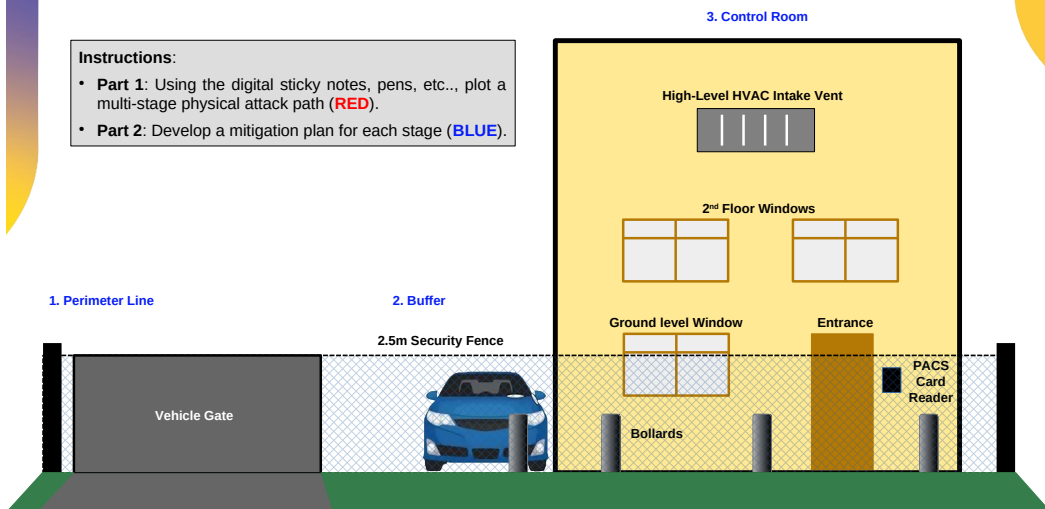
INSPIRING FUTURES

setu.ie | 40

Exercise: The Virtual Break-in

Instructions:

- **Part 1:** Using the digital sticky notes, pens, etc..., plot a multi-stage physical attack path (**RED**).
- **Part 2:** Develop a mitigation plan for each stage (**BLUE**).



Part 1: RED Team Raid

Time: 10 min

- **Breach the perimeter and knock out the OT systems.**
- **Mission:** You are an adversarial threat actor targeting this high-value facility. Working in your team, you must coordinate a multi-stage physical or environmental attack to completely disrupt operations.
- **Rules:**
 - **Plot 3 Paths:** Identify exactly three distinct vulnerabilities on your canvas.
 - **Coordinate the Attack:** Use the virtual pens or RED digital sticky notes to draw your entry paths and note your methods.
 - **Think Like a Threat:**
 - Can you exploit the environment or structure to bypass the 2.5m fence line?
 - How will you bypass the ground-level windows or tail-gate the PACS reader?
 - Can you disrupt the facility's life support systems (Power/HVAC) from the outside?

INSPIRING FUTURES

setu.ie | 42

Part 2: BLUE Team Hardning

Time: 8 min

- **Neutralise the threat vectors and reinforce the facility.**
- **Role Swap:** You are now the Lead Security Engineers for this facility.
- **Mission:** Analyse the **Red** attack paths left by the previous team and deploy exactly three targeted, cost-effective controls to stop them.
- **Rules:** Use the virtual pens or **Blue** digital sticky notes to place your defenses directly over their red attack vectors.

INSPIRING FUTURES

setu.ie | 43

Layered Physical Access Control Systems (PACS)

Control, Don't Just Block

- Standard physical barriers simply block movement; a true PACS actively dictates who, when, and for how long access is permitted.
- **The First Line** (Fencing & Approach):
 - 1 Metre: Designed to deter casual trespassers.
 - 2 Metres: Makes a quick climb difficult.
 - 2.5 Metres+: Essential for delaying a determined intruder.
- **Bollards & Clearways:** Implementing a grass or gravel clearway paired with bollards stops vehicles from parking near or ramming the perimeter line.
- **The Single-File Principle:** Turnstiles funnel patrons into single-file entry, ensuring security personnel or CCTV cameras have a completely clear view to isolate and log each person.



setu.ie | 44

Perimeter Hardening & Mantraps

Eliminating Weak Points at the Boundary

- **The Vulnerable Door:** All exterior doors must be constructed from steel, aluminium alloy, or solid-core hardwood, with at least 1.5mm steel on side and rear exits. Ensure door frames are securely fixed to the walls and outside hinges use non-removable pins.
- **Mantraps (Dead-Space Enforcement):**
 - Features a small space enclosed by two sets of interlocking doors; the first set must fully close before the second set can open.
 - Can be configured to automatically lock down and trap a suspect within the dead-space the moment an alarm is triggered.
- **Glazing Security:** Ditch standard plate glass (which shatters into hazardous shards) in favour of tempered glass (shatters into small, safe fragments) or polycarbonate glass (a thermoplastic polymer providing the toughest available glazing resistance against physical tools).



INSPIRING FUTURES

setu.ie | 45

Environmental Constraints – Power & HVAC

Securing the Digital Life Support Systems

- **Anatomy of Power Failures:** Recognise the thresholds between
 - **Sag** (momentary voltage drop),
 - **Brownout** (prolonged low voltage), and
 - **Fault/Blackout** (complete loss of power).
- **The UPS Buffer:** Instantaneous battery backup, typically running for 5–15 minutes. This is designed strictly to bridge the gap until auxiliary power comes online or to allow a clean, safe shutdown of critical OT assets.
- **HVAC & Positive Pressure:**
 - Maintains strict temperature and humidity controls to prevent critical hardware degradation.
 - **Security Enforcement:** Maintaining higher air pressure inside the facility than outside ensures that any structural leakage flows outward. A sudden drop in positive pressure serves as an immediate indicator of a door or window breach.

INSPIRING FUTURES

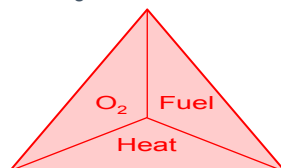
setu.ie | 46

Fire & Water Suppression in OT

Defending Without Self-Destructing

- **Fire Triangle:** Combustion requires a right mixture of Heat, Fuel, and an Oxidising Agent (O₂); removing any single element extinguishes the fire.
- **Gaseous Suppression (Control Rooms & Data Centres):**
 - **Halocarbon Gases:** Extinguish fires quickly (approx. 10 seconds) by rapidly removing heat from the area. Requires tight local storage (max 30m) and absolute evacuation before release.
 - **Inert Gases** (Argon/Inergen): Displace oxygen below the concentration needed to sustain combustion. They perform better in imperfectly sealed rooms and can be piped from 100–200m away.
- **Pre-Action Sprinkler Systems:** The safest liquid alternative. Pipes remain completely dry to avoid accidental leak damage to electronics. Water only enters the pipes when a smoke detector triggers, and will only discharge into the room once a physical temperature threshold is reached.

Ozone Depletion Potential (ODP)
Halon 1301: ODP = 10 (now banned)
Hydrofluorocarbons (HFC): ODP = 0
Inert Gases: ODP = 0



INSPIRING FUTURES

setu.ie | 47

Exercise



INSPIRING FUTURES

setu.ie | 48

Primary IT Presumption

Historically, what primary assumption did IT professionals operate under regarding their systems?

- A) Systems must maintain absolute uptime without ever being rebooted.
- B) Systems could be regularly patched, rebooted, and upgraded.
- C) Systems should rely entirely on isolated legacy protocols with multi-decade lifecycles.
- D) Systems had to prioritise human safety over data web connectivity.

Primary IT Presumption

Historically, what primary assumption did IT professionals operate under regarding their systems?

- A) Systems must maintain absolute uptime without ever being rebooted.
- B) **Systems could be regularly patched, rebooted, and upgraded.** ✓
- C) Systems should rely entirely on isolated legacy protocols with multi-decade lifecycles.
- D) Systems had to prioritise human safety over data web connectivity.

Convergence Business Drivers

What business drivers have forced the collapse of the traditional silos between IT and OT?

- A) The drive for business intelligence, predictive maintenance, and remote efficiency.
- B) The desire to replace physical valves and pumps with purely virtual applications.
- C) A mandated reduction in expected system lifecycles down to just a few months.
- D) The need to apply standard corporate patching schedules to active assembly lines.

Convergence Business Drivers

What business drivers have forced the collapse of the traditional silos between IT and OT?

- A) **The drive for business intelligence, predictive maintenance, and remote efficiency.** ✓
- B) The desire to replace physical valves and pumps with purely virtual applications.
- C) A mandated reduction in expected system lifecycles down to just a few months.
- D) The need to apply standard corporate patching schedules to active assembly lines.

PERA

What is the engineering objective of understanding PERA and mapping these controlled data flows?

- A) To extend the expected lifecycles of corporate desktop networks.
- B) To allow boardroom applications to directly override physical safety valves.
- C) To defend modern critical infrastructure using foundational engineering principles.
- D) To eliminate the need for remote efficiency and predictive maintenance.

PERA

What is the engineering objective of understanding PERA and mapping these controlled data flows?

- A) To extend the expected lifecycles of corporate desktop networks.
- B) To allow boardroom applications to directly override physical safety valves.
- C) **To defend modern critical infrastructure using foundational engineering principles. ✓**
- D) To eliminate the need for remote efficiency and predictive maintenance.

SCADA and DCS

What is the difference between a DCS and SCADA?

- A) There is no difference
- B) SCADA is designed to cover a large geographical distance
- C) SCADA systems are event driven
- D) A DCS is state driven

SCADA and DCS

What is the difference between a DCS and SCADA?

- A) There is no difference
- B) **SCADA is designed to cover a large geographical distance ✓**
- C) **SCADA systems are event driven ✓**
- D) **A DCS is state driven ✓**

Safety Instrumented Systems

Why are SIS considered "passive"?

- A) They are ineffective in an emergency
- B) They rely on a HMI to operate in an emergency
- C) They do not respond until they are called into action
- D) They do not expose the industrial environment to any threat

Safety Instrumented Systems

Why are SIS considered "passive"?

- A) They are ineffective in an emergency
- B) They rely on a HMI to operate in an emergency
- C) **They do not respond until they are called into action** ✓
- D) They do not expose the industrial environment to any threat

Learning Outcomes



Learning outcomes

You should now be able to:

- Deconstruct the industrial hardware stack, explaining the relationship between transducers, control loops, fieldbuses, and PLCs. ✓
- Compare and Contrast the operational roles, scales, and architectural boundaries of SCADA, DCS, and SIS. ✓
- Evaluate physical security perimeters, site designs, and environmental mitigation controls (HVAC, fire, power) designed to protect critical assets. ✓
- Justify why physical access control is fundamentally linked to digital integrity in an operational technology environment. ✓



Ollscoil
Teicneolaíochta
an Oirdheiscirt
South East
Technological
University



EUR ING Dr Diarmuid Ó Briain
Innealtóir Cairte agus Léachtóir Sinsearach

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



Ollscoil
Teicneolaíochta
an Oirdheiscirt
South East
Technological
University

Thank you

engcore
advancing technology

INSPIRING FUTURES