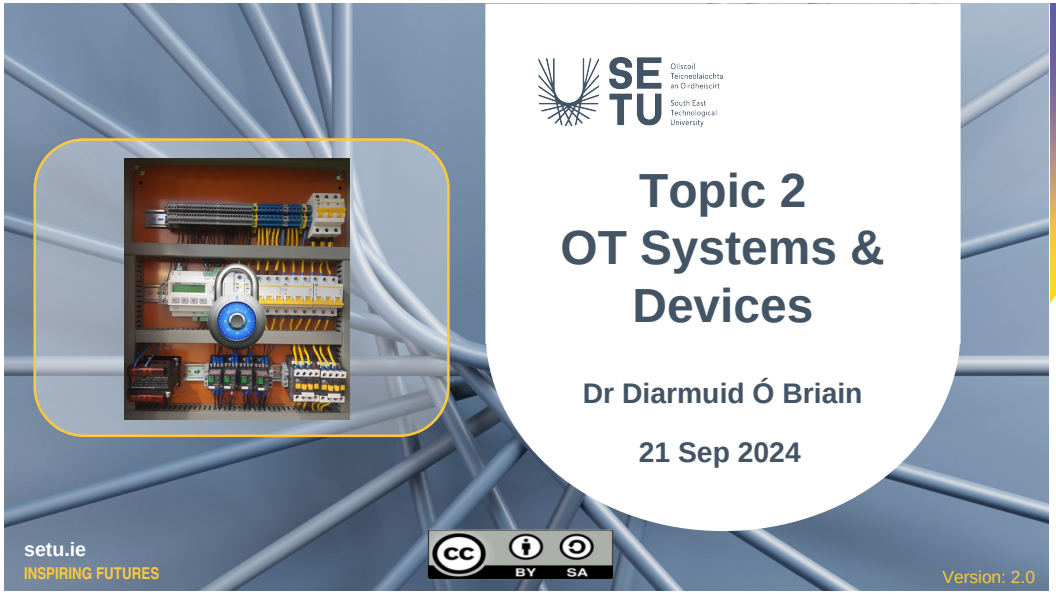


Topic 2
OT Systems & Devices

Dr Diarmuid Ó Briain

21 Sep 2024

setu.ie
INSPIRING FUTURES

Version: 2.0

Licence

Learning objectives

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

- Summarise and categorise the devices within Operational Technology (OT)
- Explain a generic security architecture that could be deployed in many areas of OT
- State that Physical Access Control Systems (PACS) are a type of physical security system designed to control access to an area.

Shannon Airport, Ireland

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:

5

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

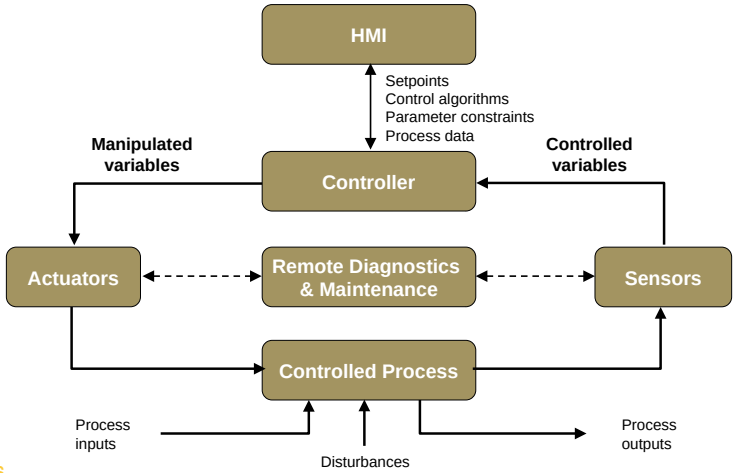
Which of the following industrial locations use OT devices?

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** ✓

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



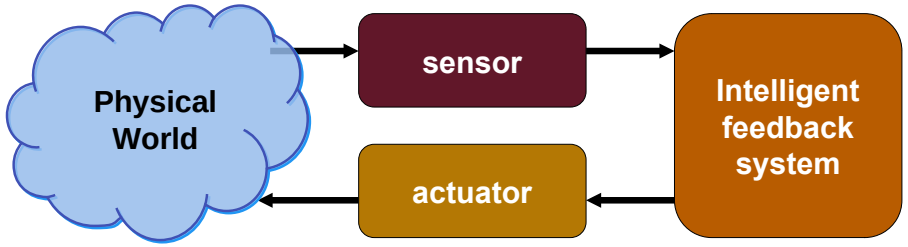
Control loops

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 mV signal representation
  - Discrete
    - Binary – boolean output (i.e. reed, proximity and photoelectric)
    - Digital – sensor converts to digital (i.e. temperature, Ph level, pressure)

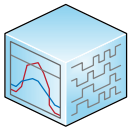
Actuators

- 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

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.



ESB BT repairing a line

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?

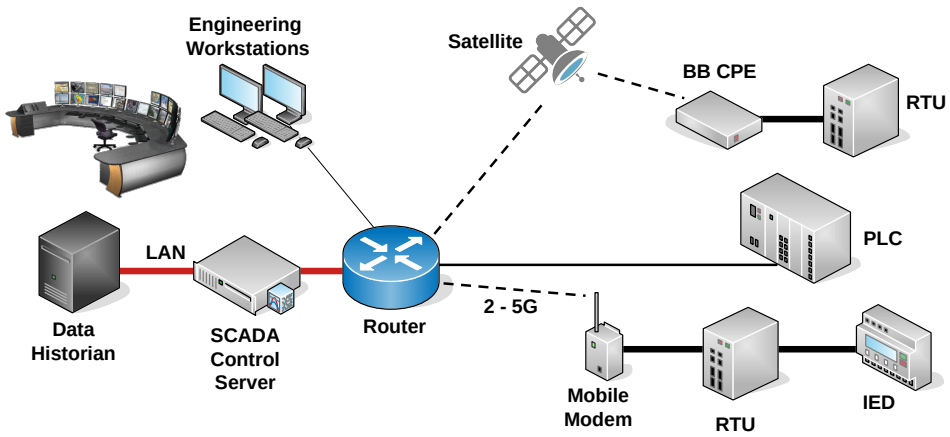
A) Flashing lights on train station signalling control boards
B) Advancements in IoT
C) Ethernet & Internet connectivity
D) Physical control switches

SCADA and vulnerabilities

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

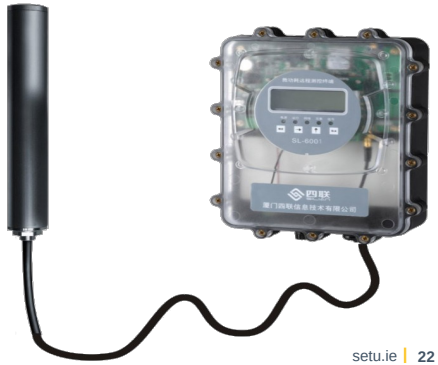
A) Flashing lights on train station signalling control boards
B) **Advancements in IoT** ✓
C) **Ethernet & Internet connectivity** ✓
D) Physical control switches

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.

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 (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

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

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 controlled by PLCs?

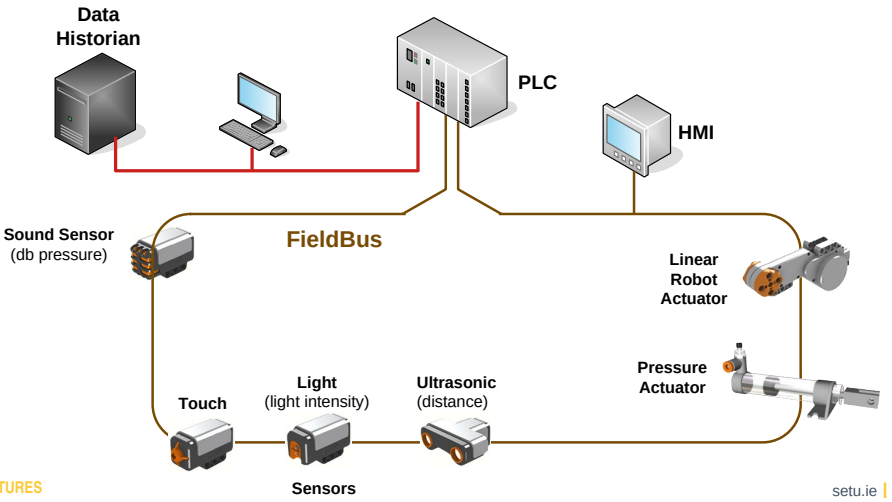
A) Temperature sensor
B) Robot arm actuator
C) Pressure valve
D) Fire hose
E) None of the above

PLC control

Which of the following is NOT an example of something controlled by PLCs?

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

PLC Control System



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 Neworking (TSN)
D) None of the above

Fieldbus

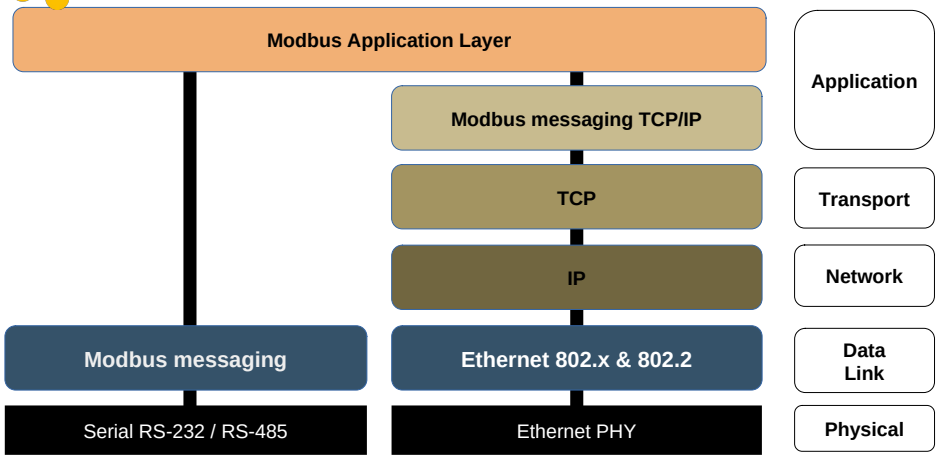
Which of the following are considered a Fieldbus?

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.

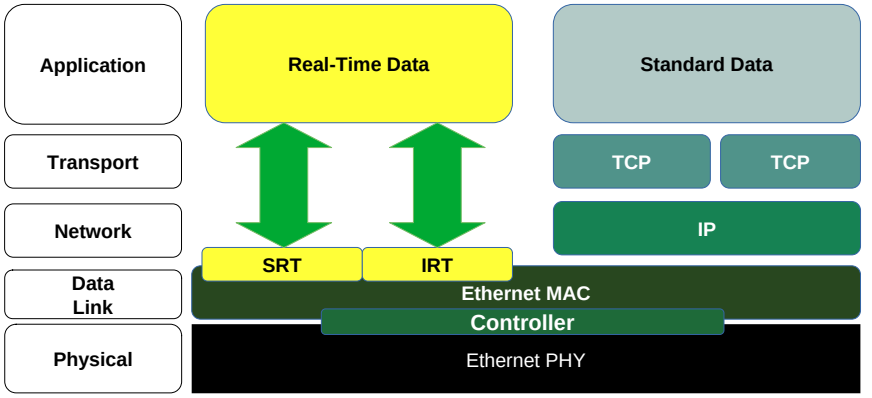
Modbus



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.

PROFINET®



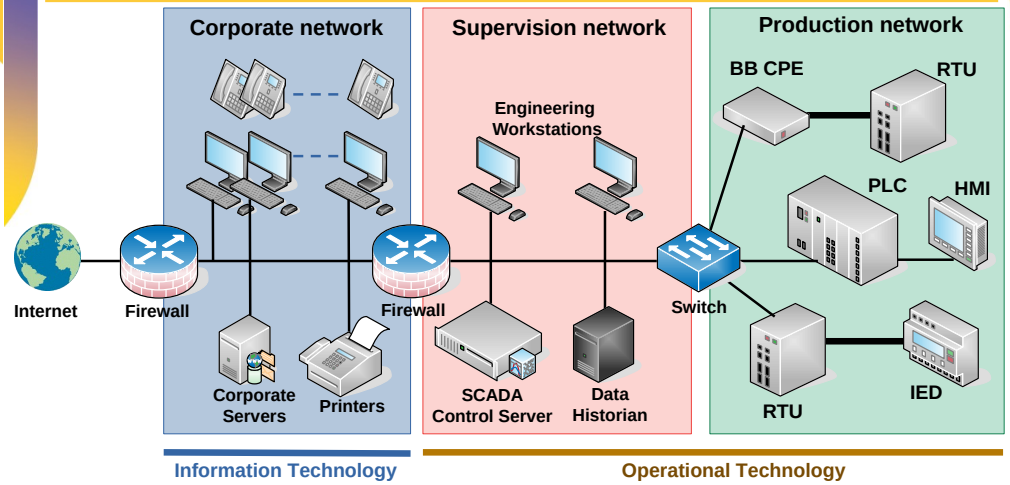
SIEMENS

Physical Access Control Systems (PACS)

- Physical security system designed to control access to an area.
- Unlike standard physical barriers, physical access control can control who is granted access, when the access is granted, and how long the access should last.




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

OT in use

- Use the audit worksheet below to identify how the systems at the airport that you identified earlier and their related devices play a role in the airport OT.

OT/Device	User(s)	Use	Connection	Application	Vulnerabilities

Learning outcomes

You should be able to:

- Summarise and categorise the devices within OT ✓
- Explain a generic security architecture that could be deployed in many areas of OT ✓
- State that PACS are a type of physical security system designed to control access to an area ✓

TUS
Ollscoil Teicneolaíochta na Sionainne: Lár Tíre, An Iarthar Láir
Technological University of the Shannon: Midlands Midwest

EUR ING Dr Diarmuid Ó Briain
Innealtóir Cairte agus Léachtóir Sinsearach

E diarmuid.obriain@tus.ie | W tus.ie
Campas Maoilis, Páirc Maoilis,
Luimneach, V94 EC5T, Éire

CEng, FIEI
CISSP®

Thank you

TUS