# Topic 2

# Operational Technology Systems and Devices

**Dr Diarmuid Ó Briain**

**Version: 2.0**

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

**Dr Diarmuid Ó Briain**

# Table of Contents

# Illustration Index

# 1 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
- Physical Access Control Systems (PACS) are a type of physical security system designed to control access to an area.

# 2 Introduction

This is an introduction to OT devices and how they interact with the world. This topic will go through each of these devices, how they are configured, not only a industrial space but also consider some real-world context in how they interact with the real world.


*Figure 1: Consider OT devices at an airport*

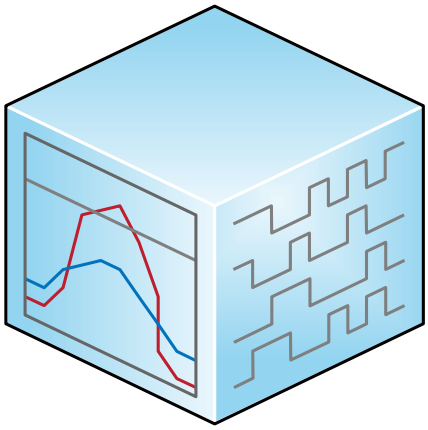

*Figure 2: SCADA*

# 3 Typical OT System

OT systems consist of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an ***objective***, such as, manufacturing, transportation or energy). 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 control components of the system include the specification of the desired output or performance.

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.

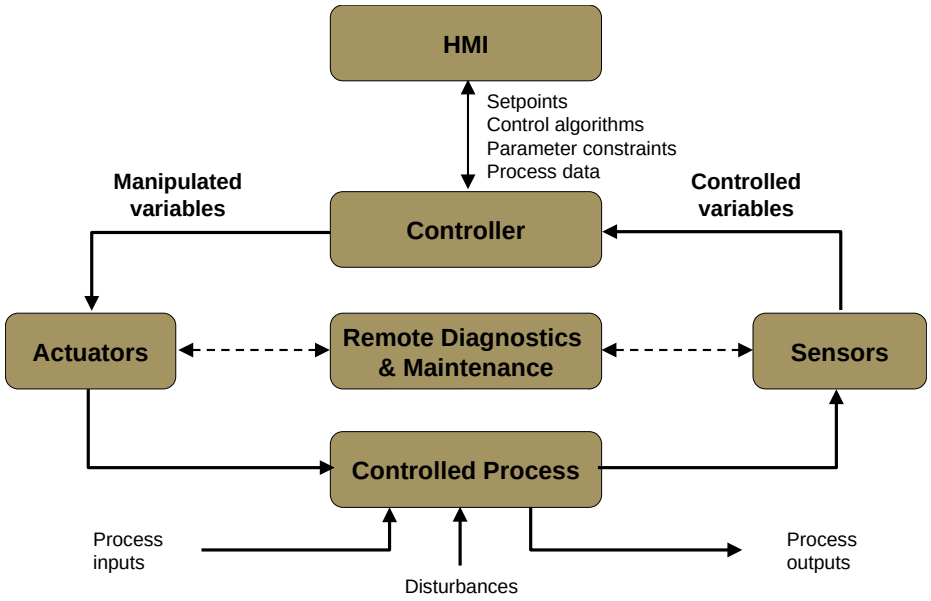


*Figure 3: Typical OT System*

Figure 3 depicts, a typical OT system that contains numerous control loops, Human Machine Interfaces (HMI), and Remote Diagnostics & Maintenance (RDM) tools. The system is built using an array of network protocols on layered network architectures. Some critical processes may also include safety systems.

A control loop utilises sensors, actuators, and controllers to manipulate some controlled process. A ***sensor*** is a device that produces a measurement of some physical property and then sends this information as controlled variables to the controller. The ***controller*** interprets the signals and generates corresponding manipulated variables, based on a control algorithm and target set-points, which it transmits to the actuators. ***Actuators*** such as control valves, breakers, switches, and

motors are used to directly manipulate the controlled process based on commands from the controller.

Operators and engineers use HMIs to monitor and configure set-points, control algorithms, and adjust and establish parameters in the controller. The HMI also displays process status information and historical information. Diagnostics and maintenance utilities are used to prevent, identify, and recover from abnormal operation or failures.

## 3.1 Control loops

Sometimes control loops are nested and/or cascading, whereby the set point for one loop is based on the process variable determined by another loop. Supervisory-level loops and lower-level loops operate continuously over the duration of a process, with cycle times ranging on the order of milliseconds to minutes.

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**. System processes have a wide range of time-related requirements, including very high speed, consistency, regularity, and synchronisation. Humans may not be able to reliably and consistently meet these requirements; automated controllers may be necessary. Some systems may require computation to be performed as close to sensors and actuators as possible to reduce communication latency and perform necessary control actions on time.
- **Geographic Distribution**. Systems have varying degrees of distribution, ranging from a small system to large, distributed systems. Greater distribution typically implies a need for wide area networking and mobile communication.
- **Hierarchy**. Supervisory control is used to provide a central location that can aggregate data from multiple locations to support control decisions based on the current state of the system. Often a hierarchical/centralised control is used to provide human operators with a comprehensive view of the entire system.
- **Control Complexity**. Often control functions can be performed by simple controllers and preset algorithms. However, more complex systems require human operators to ensure that all control actions are appropriate for meeting the larger objectives of the system.
- **Availability**. Reliability requirements of the system are also an important factor in design. Systems with strong availability/up-time requirements may require more redundancy or alternate implementations across all communications and control.
- **Impact of Failures**. The failure of a control function could cause substantially different impacts across domains. Systems with greater impacts often require the ability to continue operations through redundant controls or to operate in a degraded state. The design needs to address these requirements.
- **Safety**. The system's safety requirements are an important factor in design. Systems must be able to detect unsafe conditions and trigger actions to reduce unsafe conditions to safe ones. In most safety-critical operations,

human oversight and control of a potentially dangerous process is an essential part of the safety system.

## 3.2 Transducers

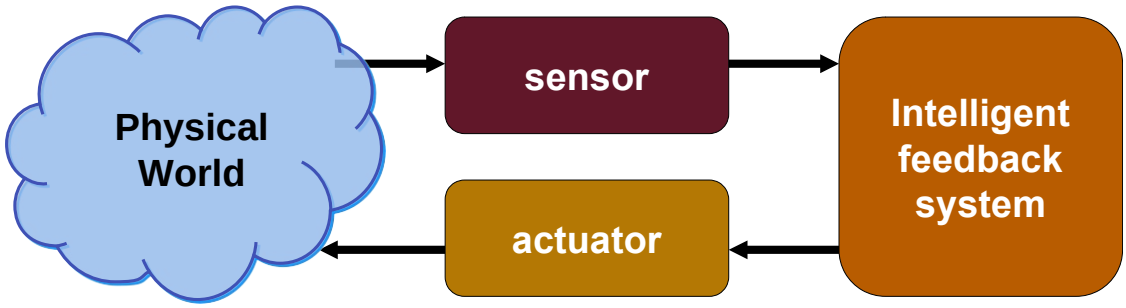


*Figure 4: Transducers*

A transducer is a device that converts a primary form of energy into a corresponding signal with a different energy form. There are many primary energy forms such as mechanical, thermal, electromagnetic, optical, chemical, etc. To interact with these primary forms it is necessary to detect with a sensor and generate with an actuator.

Sensors (e.g., thermometer) are devices that detect/measure a signal or stimulus acquires information from the “real world” whereas an actuator (e.g., heater) is a device that generates a signal or stimulus.

### 3.2.1 Sensors


*Figure 5: Examples of sensors*

A sensor is a transducer that converts a physical stimulus from one form into a more useful form to measure the stimulus. There are some examples in Figure 5, They come in two basic categories:

- **Analogue sensors**
  - These convert the environmental input into output analogue signals, which are continuous and varying. Thermocouples that are used in gas hot water heaters offer a good example of an analogue sensor. The water heater's pilot light continuously heats the thermocouple. These analogue signals are typically represented by a voltage signal between 4 – 20 mV.

- **Discrete sensors**
  - Discrete sensors send high/low, on/off or yes/no signals to a controller regarding the quantity of a physical parameter. These can be further broken into binary, and Digital discrete sensors. Discrete sensors have an advantage over analogue sensors due to the absence of deadband, detection speed, analogue thresholds and other similar complexities. They are also more suitable for operation with microprocessors.
  - **Binary**
    - Binary sensors, whose output is in boolean form, that is they sense one of two possible values according to whether the sensed variable exceed or not a given threshold. Limit switches, Reed switches, Proximity switches and Photoelectric or photo eye sensors are some examples.
  - **Digital**
    - Digital sensors have been developed to overcome the traditional disadvantages of analogue sensors. Such sensors take analogue inputs and directly convert them to a digital signal inside the sensor. Therefore instead of voltage signal levels from 4 – 20 mV a digital data signal is sent. This digital data transmission is unaffected by cable length, cable resistance or impedance, and is not influenced by electromagnetic noise. Examples of digital sensors include temperature, Ph level, pressure, gyroscope, compass and tilt/acceleration sensors.

### 3.2.2 Actuators

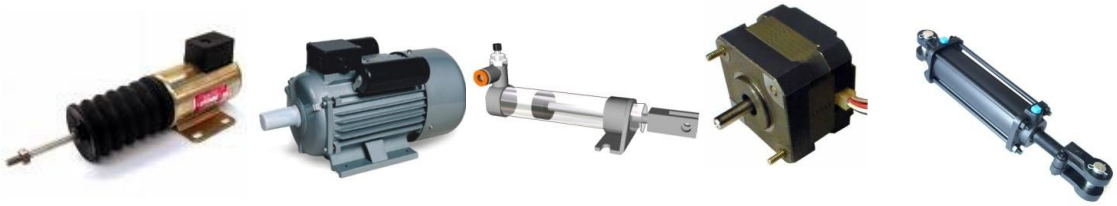

*Figure 6: Examples of Actuators*

An actuator is a component of a machine that is responsible for moving and controlling a mechanism or system, for example by opening a valve. These can be broken into Electrical, Hydraulic and Pneumatic actuators. Electrical actuators include Electric motors and solenoids. Hydraulic actuators use hydraulic fluid to amplify the controller command signal while pneumatic actuators use compressed air as a driving force.

# 4 Supervisory Control and Data Acquisition

Supervisory Control and Data Acquisition (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.

SCADA systems are event driven in that they respond to events that occur in the process they are monitoring and controlling. Events can be generated by sensors, actuators, or even other SCADA systems.

For example, a SCADA system might monitor the pressure in a pipeline. If the pressure falls below a certain threshold, the SCADA system might generate an event and send an alarm to the operator. The operator could then take action to correct the problem.

SCADA systems can also be used to implement more complex event-driven control logic. For example, a SCADA system might be used to control the traffic signals at a busy intersection. The SCADA system would monitor the traffic sensors at the intersection and generate events when the traffic flow changes. The SCADA system would then use these events to determine the appropriate timing for the traffic signals.

Event-driven SCADA systems have a number of advantages over traditional polling-based SCADA systems. Event-driven systems are more efficient, as they only need to process data when an event occurs. This can be especially important for large and complex SCADA systems. Event-driven systems are also more responsive, as they can respond to events immediately. This can be important for critical applications, such as traffic control and power generation.

Introducing new communications technology to legacy SCADA systems to try to get them more connected and leverage the data within the system with each other and get them all sort of communicating properly with each other to get the data out of them. This presents security issues were with that scenario. There is a lot of potential for things to go wrong. Alarms could be missed because the new technology is not connecting with the old technology for example.

Older technology may require an operator oversight to watch for a flashing light indicator. Or if there has not been adequate training between the two, perhaps it may even be a loss of legacy knowledge. Essentially the biggest risk is people and process. Training issues, as well as awareness is essential because with the convergence of IT and OT, security and training are key components to ensure success. Without out that there are many factors of concern.

Example: Consider Conor a Network Technician (NT) within the Electricity Supply Board (ESB).

*Figure 7: ESB Network Technician (NT) attending a line break at a tree fall*

A tree falls on a line and locals report that sparks are coming from the area and a heavy duty wire is jumping around. In the past an 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. This of course could take time. With SCADA, the system can immediately trip the breaker at the feeding sub-station to make the line safe, though that will remove power from all customers connected to that line. However, the situation is safe and 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 suffering from power outage but not impacted by the problem on the spur.

## 4.1 OT Architecture

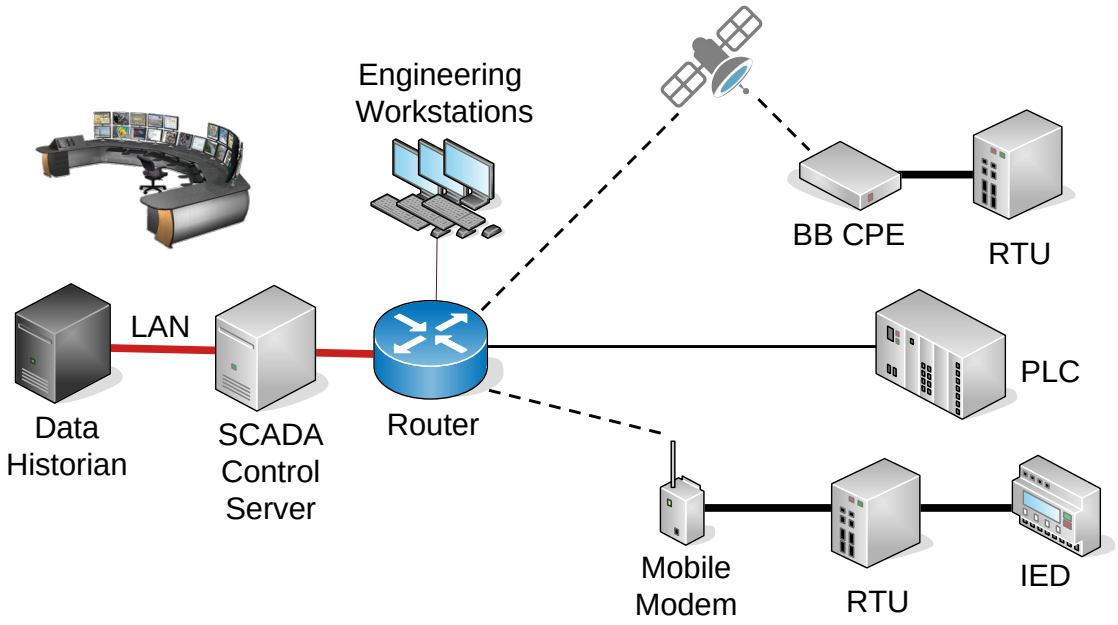


*Figure 8: SCADA Architecture*

Figure 8 illustrates the components and general configuration of a OT system. The control centre houses a control server and the communications routers. Other control centre components include the HMI, engineering workstations, and the data historian, which are all connected by a LAN. The processes at the control centre collects and logs information gathered by the field sites, displays information to the HMI, and may generate actions based upon detected events. The control centre is also responsible for centralised alarming, trend analyses, and reporting.


*Figure 9: RTU and IED*

Additionally the control centre has communications equipment (e.g., radio, fibre, cable, or satellite) to connect with one or more geographically distributed field sites consisting of Remote Terminal Units (RTU) and/or Programmable Logic Controllers (PLC), which control actuators and/or monitor sensors. In the case of the RTU it transmits telemetry data to the master system, and respond to messages from the master supervisory system to control connected objects.

The control server stores and processes the information from RTU inputs and outputs, while the RTU or PLC controls the local process. The communications hardware allows the transfer of information and data back and forth between the control server and the RTUs or PLCs.

The software is programmed to instantiate processes that monitor devices and process, what parameter ranges are acceptable, and what response to initiate when a process variable changes outside acceptable values.

An Intelligent Electronic Device (IED), such as a protective relay, may communicate directly to the control server, or a local RTU may poll the IEDs to collect the data and pass it to the control server. IEDs provide a direct interface to control and monitor equipment and sensors. Such IEDs may be directly polled and controlled by the control server and in most cases have local programming that allows for the IED to act without direct instructions from the control centre.

SCADA systems are usually designed to be fault-tolerant systems with significant redundancy built into the system, although redundancy may not be a sufficient countermeasure in the face of malicious attack.

# 5 Distributed Control Systems

While SCADA is centralised, Distributed Control Systems (DCS) is 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.

DCS are state driven. This means that they continuously monitor the state of the process they are controlling and take actions based on that state. For example, a DCS might monitor the temperature of a reactor and adjust the flow of cooling water to keep the temperature within a safe range.

DCS are typically designed with a hierarchical structure, with each level of the hierarchy responsible for a specific set of tasks. The lowest level of the hierarchy is made up of field controllers, which are devices that directly interface with the process sensors and actuators. Field controllers are responsible for collecting data from the sensors and sending it to the next level of the hierarchy, which is typically a process controller.

Process controllers are responsible for implementing the control logic for the process. They use the data collected from the field controllers to calculate the desired values for the actuators. The process controllers then send these values to the field controllers, which adjust the actuators accordingly.

The highest level of the hierarchy is typically a supervisory controller. The supervisory controller is responsible for monitoring the overall performance of the process and making adjustments to the control logic as needed.

DCS use a variety of communication protocols to connect the different levels of the hierarchy. Common protocols include Ethernet, Modbus, and ProfiNet.

DCS are used in a wide variety of industries, including oil and gas, petrochemicals, power generation, and manufacturing. They are particularly well-suited for complex processes that require a high degree of control.

# 6 Safety Instrumented Systems

*Figure 10: Fire Suppression System*

Another OT system to take into account is Safety Instrumented Systems (SIS). These are dormant systems, or passive systems, and they do not respond until they are called into action. An example is 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 in case the operational and safety threshold is exceeded, which could result in an explosion.

There are a lot of these type of OT systems and they are very important to consider by security professionals because they can cause loss of life, or they create another threat vector in which bad actors can use them to again, cause production loss and or loss of life.

Figure 10 illustrates a Fire Suppression System, an SIS that remains dormant until the occurrence of a fire.

# 7 Programmable Logic Controller

*Figure 11: Siemens SIMATIC S7 Controller*

PLCs are used in both SCADA and DCS systems as the control components of an overall hierarchical system to provide local management of processes through feedback control. In the case of SCADA systems, they may provide similar functionality to RTUs. When used in DCS, PLCs are implemented as local controllers within a supervisory control scheme. In addition to PLC usage in SCADA and DCS, PLCs can be implemented as the primary controller in smaller OT system configurations to provide operational control of discrete processes. These topologies differ from SCADA and DCS in that they generally lack a central control server or HMI and, therefore, primarily provide *closed-loop* control with minimal human involvement. PLCs have a user programmable memory for storing instructions for the purpose of implementing specific functions such as I/O control, logic, timing, counting, three mode Proportional-Integral-Derivative (PID) control, communication, arithmetic, and data and file processing.

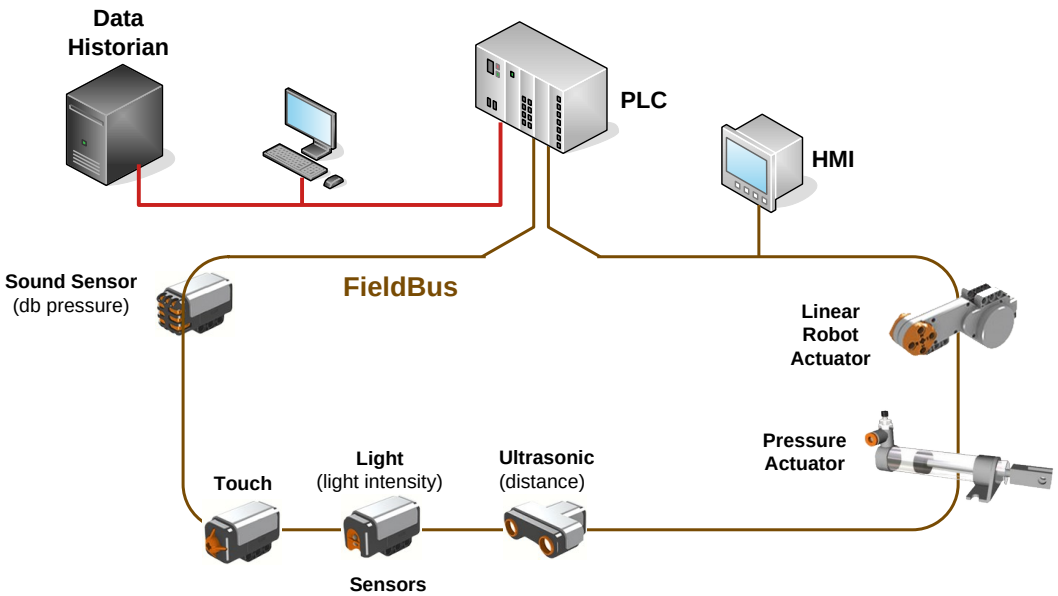


*Figure 12: PLC Control System*

## 7.1 Fieldbus

A fieldbus is an industrial digital communication network used for real-time distributed control. A complex automated industrial system is typically structured in hierarchical levels as a DCS. In this hierarchy the upper levels for production managements are linked to the direct control level of PLCs via a non-time-critical communications system, such as Ethernet. The fieldbus links the PLCs of the direct control level to the components in the plant of the field level such as sensors, actuators, electric motors, console lights, switches, valves and contactors and replaces the direct connections via current loops or digital I/O signals. The requirement for a fieldbus are therefore time-critical and cost sensitive, deterministic technologies such as the Time-Sensitive Networking (TSN) Ethernet extension meet this requirement.

A fieldbus works on a network structure in one of daisy-chain, star, ring, branch, and tree network topologies. Previously, computers were connected using RS-232, serial connections by which only two devices could communicate using a 4–20 mA communication scheme. As the fieldbus require only one communication point at the controller level and allows multiple analogue and/or digital points to be connected to it at the same time, there is a major reduction in both the number and the length of the cable required. Additionally, since devices that communicate through a fieldbus require a microprocessor, multiple points are typically provided by the same device. Some fieldbus devices now support control schemes such as PID control on the device side instead of forcing the controller to do the processing.

### 7.1.1 Modbus

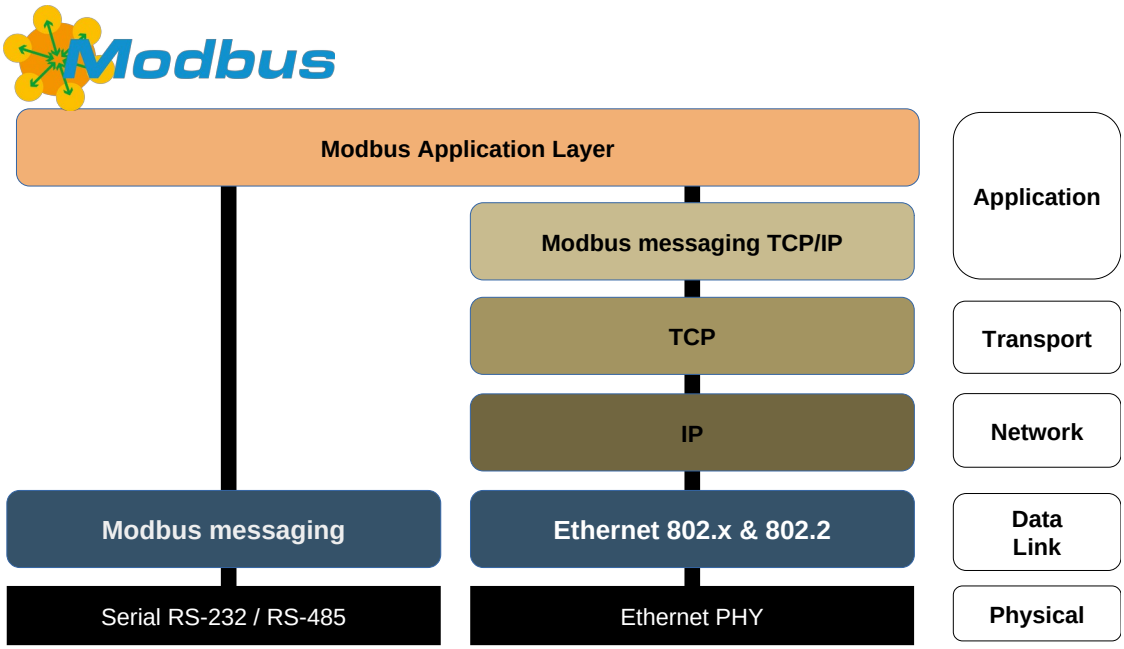


*Figure 13: Modbus Protocols*

Modbus and Modbus Transmission Control Protocol (TCP)/Internet Protocol (IP) (Modbus TCP) are two variants of the Modbus family of simple, vendor-neutral communication protocols intended for supervision and control of automation

equipment. Modbus is a serial protocol while Modbus TCP is an adaption of the protocol for transport over TCP/IP networks. Modbus itself consists of Modbus messaging in an intranet environment . The most common use of the protocols at this time is for Ethernet attachment of PLCs, I/O modules and gateways to other simple field buses or I/O networks. The Modbus TCP/IP protocol is published as a de-facto automation standard [1].

### 7.1.2 Profinet

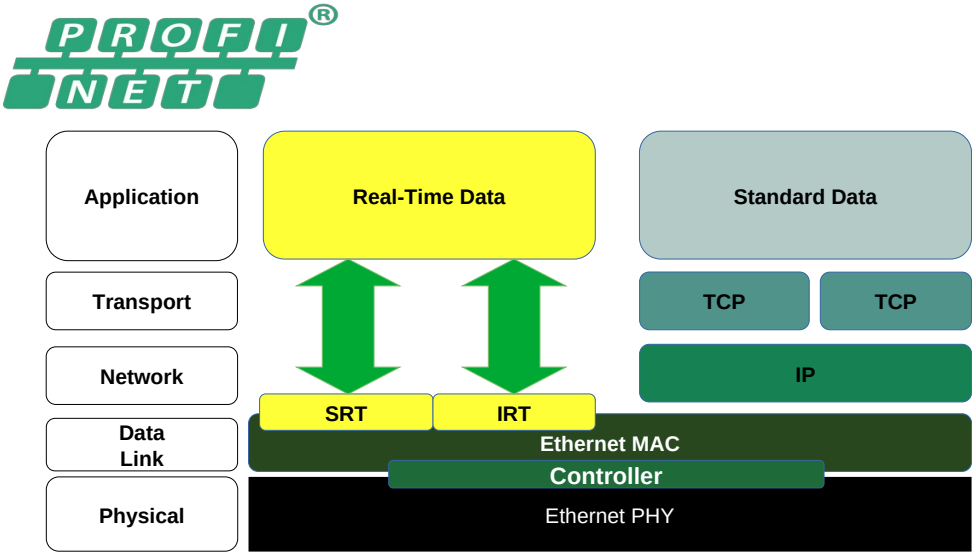


*Figure 14: Profinet protocols*

Process Field Network (Profinet) is an industry technical standard for data communication over Industrial Ethernet, designed for collecting data from, and controlling equipment in industrial systems, with a particular strength in delivering data under tight time constraints. Profinet fieldbus profiles are standardised by the International Electrotechnical Commission (IEC) as IEC 61784/61158 [2] [3].

Profinet implements the interfacing to peripherals. It defines the communication with field connected peripheral devices. Its basis is a cascading real-time concept. Profinet defines the entire data exchange between controllers and the devices, as well as parameter setting and diagnosis. IO-Controllers, such as PLC, DCS, or Industrial PC (IPC) and Devices can be varied and include I/O blocks, drives, sensors, or actuators. The Profinet protocol is designed for the fast data exchange between Ethernet-based field devices and follows the provider-consumer model.

ProfiNet Soft-Real Time (SRT) handles the time-critical data exchange functioning in the way that when an SRT frame arrives in the destination node, the frame is 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 31.25 µs and 1µs of jitter.

# 8 Physical Access Control Systems

*Figure 15: Examples of PACS*

Physical Access Control Systems (PACS) are a type of 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.

An access point is the entrance/barrier where access control is required. Some common physical access control examples of access points are doors and locks, security gates, turnstiles, and vehicular gate arms. Depending on the type of facility there can be a single access point or many.

An IDentification (ID) or personal credential is used to identify the authorised user trying to gain access to the area or facility. Most PACS require a user to have credentials to gain entrance to a facility or access sensitive data. Examples of identification credentials include simple controls (e.g., PIN codes, passwords, key fobs, key cards) and more advanced credentials (e.g., encrypted badges, mobile credentials). Identification credentials allow the system to know who is attempting to gain access and to maintain access logs.

# 9 IT/OT Architecture

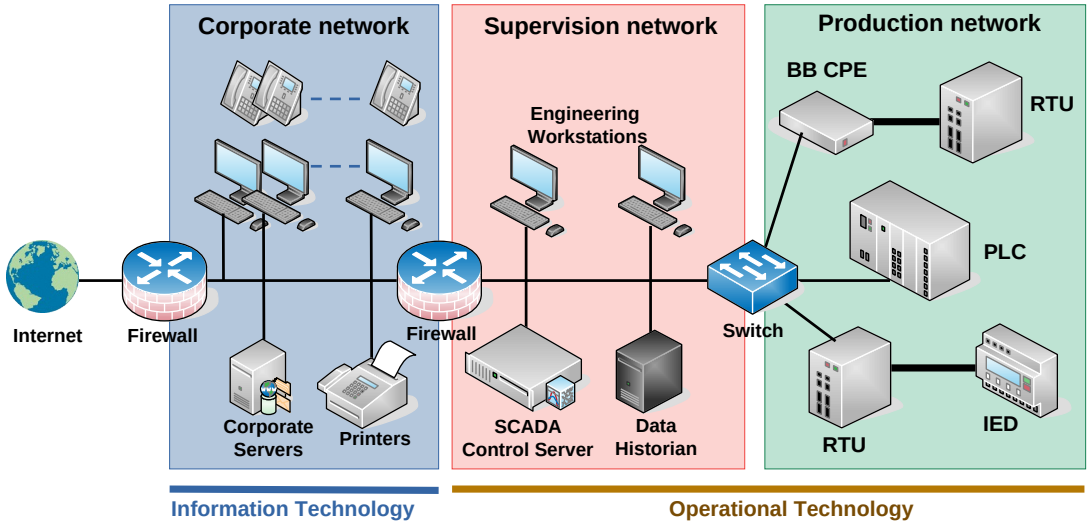


*Figure 16: OT Architecture*

Consider the OT generic architecture illustrated in Figure 16.

## 9.1 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 IEDs, 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.

## 9.2 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.

## 9.3 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 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.

## 9.4 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.

### 9.4.1 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.

## 9.5 Differences between IT and OT

The following lists some special considerations when considering security for OT [4]:

| Category | IT | OT |
|---|---|---|
| **Performance Requirements** | • Non-real time.<br>• Response must be consistent.<br>• High throughput is demanded.<br>• High delay and jitter may be acceptable.<br>• Emergency interaction is less critical.<br>• Tightly restricted access control can be implemented to the degree necessary for security. | • Real-time.<br>• Response is time-critical.<br>• Modest throughput is acceptable.<br>• High delay and/or jitter is not acceptable.<br>• Response to human and other emergency interaction is critical.<br>• 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.<br>• 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.<br>• Availability requirements may necessitate redundant systems.<br>• Outages must be planned and scheduled days/weeks in advance.<br>• High availability requires exhaustive pre- deployment testing. |

| Category | IT | OT |
|---|---|---|
| **Risk management requirements** | • Manage data.<br>• Data confidentiality and integrity is paramount.<br>• Fault tolerance is less important – momentary downtime is not a major risk.<br>• Major risk impact is delay of business operations. | • Control physical world.<br>• Human safety is paramount, followed by protection of the process.<br>• Fault tolerance is essential; even momentary downtime may not be<br>• acceptable.<br>• Major risk impacts are regulatory non-<br>• compliance, environmental impacts, and loss of life, equipment, or production. |
| **System operation** | • Systems are designed for use with typical OSs.<br>• 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.<br>• Primarily wired networks with some localised wireless capabilities.<br>• 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. |

*Figure 17: Differences between IT and OT*

# 10 Bibliography

[1] ‘MODBUS Messaging on TCP/IP Implementation Guide V1.0b’. Modbus Organization, Oct. 26, 2006. Accessed: Aug. 08, 2023. [Online]. Available: https://www.modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf

[2] IEC 61784, ‘Industrial communication networks - Fieldbus specifications - Part 1: Overview and guidance for the IEC 61158 and IEC 61784 series’. Mar. 22, 2023.

[3] IEC 61158, ‘Industrial networks - Profiles - Part 1-0: Fieldbus profiles - General concepts and terminology’. Mar. 16, 2023.

[4] K. Stouffer *et al.*, ‘Guide to Operational Technology (OT) Security’, National Institute of Standards and Technology, NIST SP 800-82 Rev. 3, Sep. 2023. Accessed: Oct. 01, 2023. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-82r3