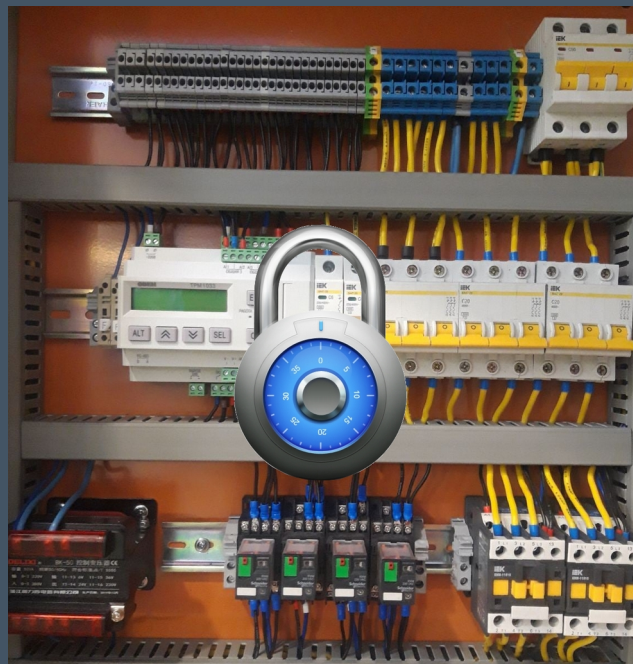


Topic 2

Hardening OT Components & Physical Boundaries



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.....	5
2 Introduction.....	5
3 The OT Hardware Stack.....	6
3.1 Typical OT System.....	6
3.2 Control loops.....	7
3.3 Transducers.....	8
3.4 Programmable Logic Controller.....	10
3.5 PLC and Ladder Logic.....	11
3.6 Fieldbus.....	11
4 Industrial Systems Scaling.....	14
4.1 Supervisory Control and Data Acquisition.....	14
4.2 SCADA and DCS.....	15
4.3 OT Architecture.....	16
4.4 Distributed Control Systems.....	18
4.5 Safety Instrumented Systems.....	19
4.6 Comparison SCADA/DCS/SIS.....	20
5 Physical Site Perimeter Defences.....	21
5.1 Physical Access Control Systems.....	21
5.2 Site and Facility Design.....	21
5.3 Secure Facility Plan & Physical Security Controls.....	22
5.4 Physical Access Controls.....	23
5.5 Perimeter Security.....	26
6 Environmental Constraints.....	29
6.1 Power.....	29
6.2 Water and Fire.....	30
6.3 Water threat.....	32
6.4 Heating, Ventilating, and Air Conditioning.....	32
7 Bibliography.....	33

Table of Figures

Figure 1: Typical OT System.....	6
Figure 2: Transducers.....	8
Figure 3: Examples of sensors.....	8
Figure 4: Examples of Actuators.....	9
Figure 5: Siemens SIMATIC S7 Controller.....	10
Figure 6: PLC Control System.....	10
Figure 7: Ladder Logic.....	11
Figure 8: Modbus Protocols.....	12
Figure 9: Profinet protocols.....	13
Figure 10: ESB Network Technician (NT) attending a line break at a tree fall.....	15
Figure 11: SCADA Architecture.....	16
Figure 12: RTU and IED.....	17
Figure 13: Fire Suppression System.....	19
Figure 14: Examples of PACS.....	21
Figure 15: Motion detector.....	23
Figure 16: CCTV.....	24
Figure 17: Turnstyle.....	27
Figure 18: Mantrap.....	28
Figure 19: Fire triangle.....	30
Figure 20: Fire Classes.....	30

Index of Tables

Table 1: Comparison between SCADA and DCS.....	16
Table 2: Comparison SCADA/DCS/SIS.....	20
Table 3: Access Log.....	25

1 Objectives

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

- Deconstruct the industrial hardware stack, explaining the relationship between transducers, control loops, fieldbuses, and Programmable Logic Controllers (PLC).
- Compare and Contrast the operational roles, scales, and architectural boundaries of Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), and Safety Instrumented Systems (SIS).
- Evaluate physical security perimeters, site designs, and environmental mitigation controls (Heating, Ventilating, and Air Conditioning (HVAC), fire, power) designed to protect critical assets.
- Justify why physical access control is fundamentally linked to digital integrity in an operational technology environment.

2 Introduction

This topic is an exploration of the physical layer of Operational Technology (OT) security. This session moves from the operational logic of internal hardware components up to the physical perimeters and environmental support systems required to keep industrial environments safe, resilient, and secure.

3 The OT Hardware Stack

3.1 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.

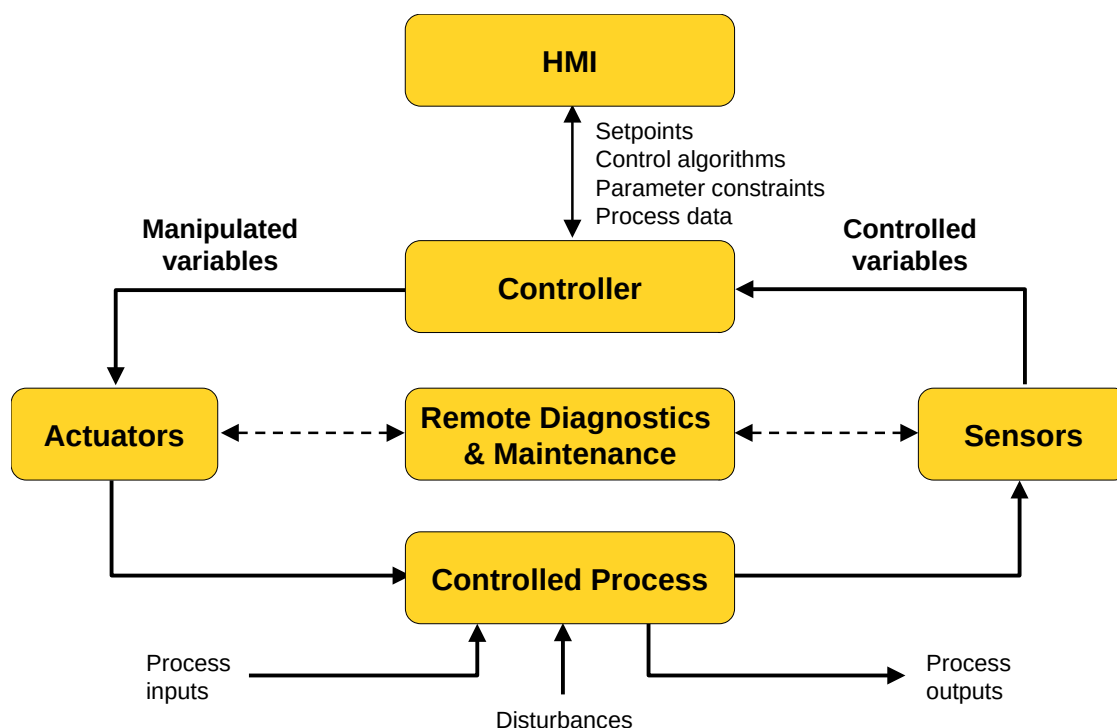


Figure 1: Typical OT System

Figure 1 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.

3.2 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.

3.3 Transducers

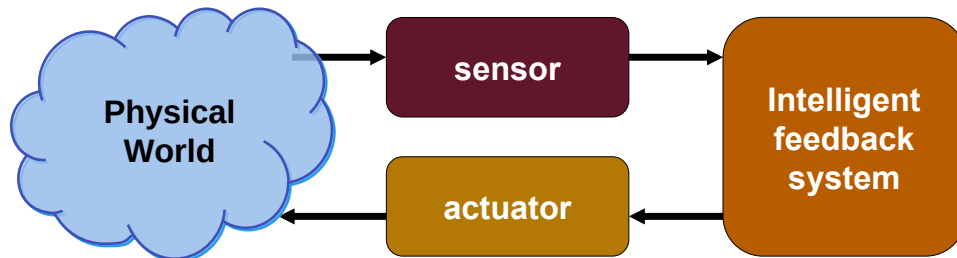


Figure 2: Transducers

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.

3.3.1 Sensors

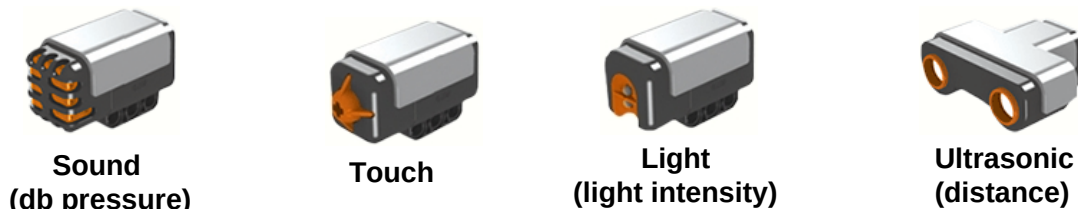


Figure 3: Examples of sensors

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 3, 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 mA.

- **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 mA 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.

3.3.2 Actuators

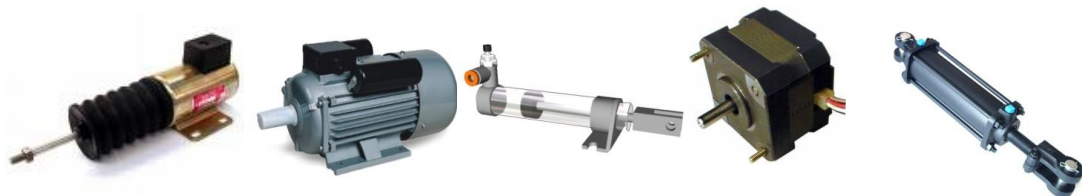


Figure 4: Examples of Actuators

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.

3.4 Programmable Logic Controller



Figure 5: 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 Remote Terminal Units (RTU). 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 Input/Output (I/O) control, logic, timing, counting, three mode Proportional-Integral-Derivative (PID) control, communication, arithmetic, and data and file processing.

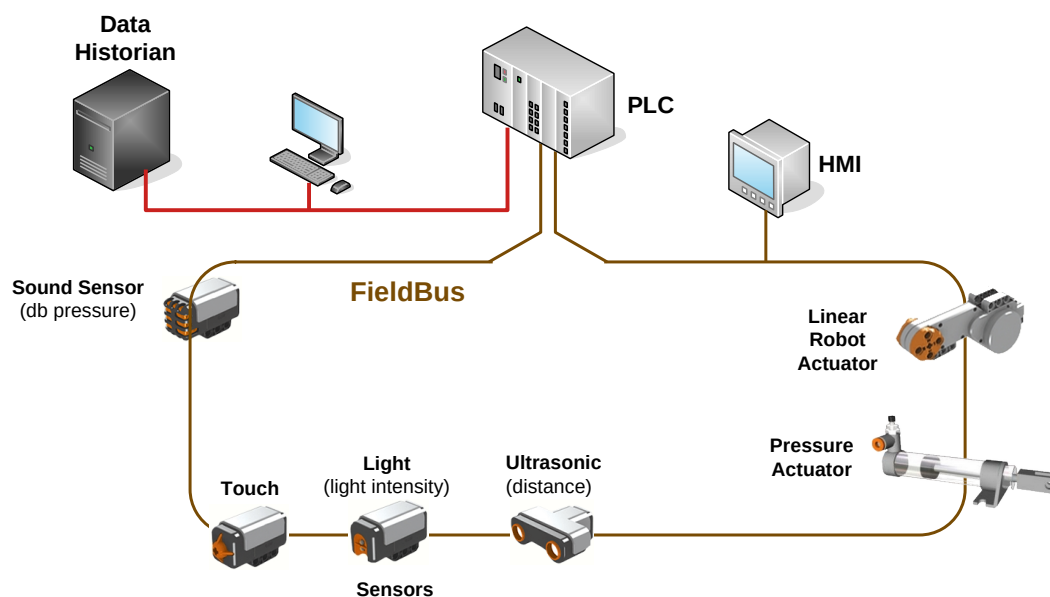


Figure 6: PLC Control System

3.5 PLC and Ladder Logic

When learning how PLCs work, it is helpful to first gain a solid understanding of ladder logic. Ladder logic is, and has always been, the principle means of programming a PLC.

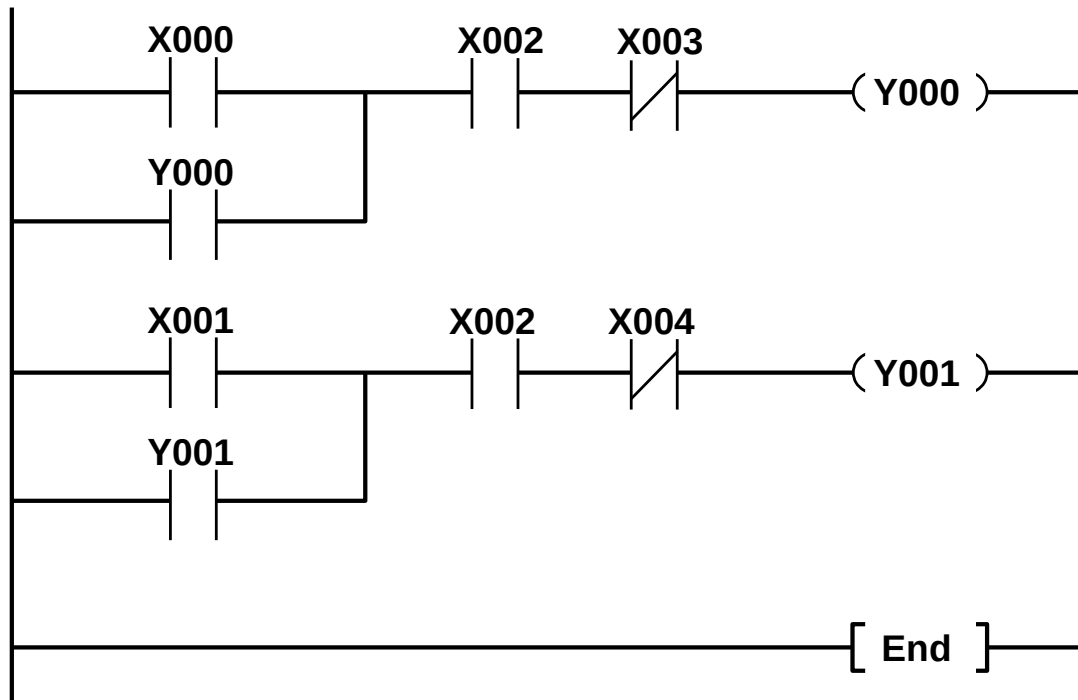


Figure 7: Ladder Logic

3.6 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.

3.6.1 Modbus

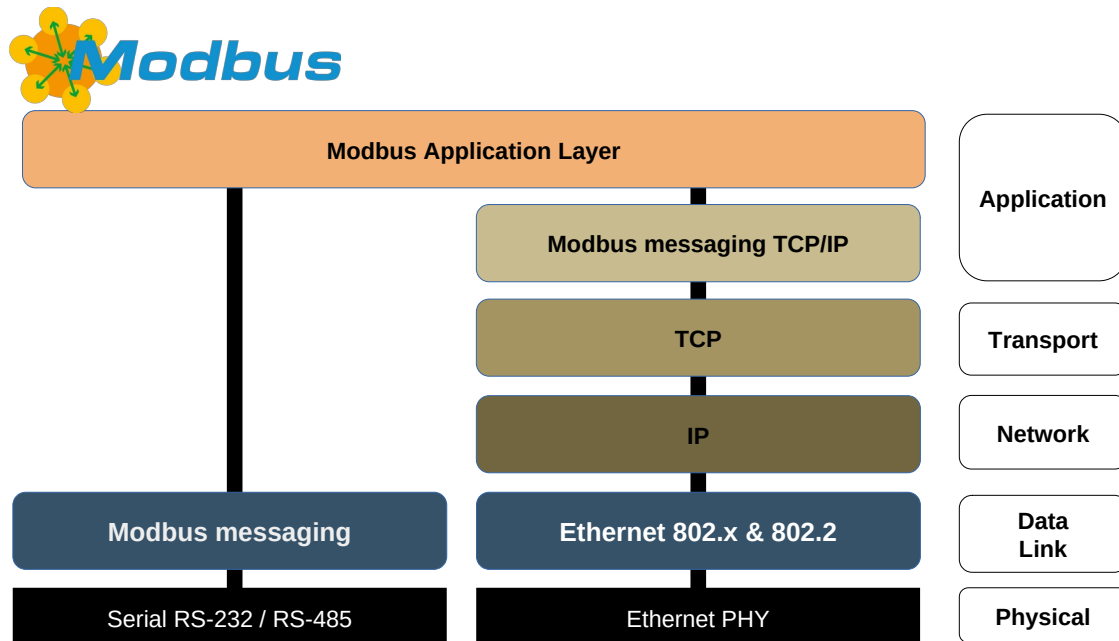


Figure 8: Modbus Protocols

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].

3.6.2 Profinet

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].

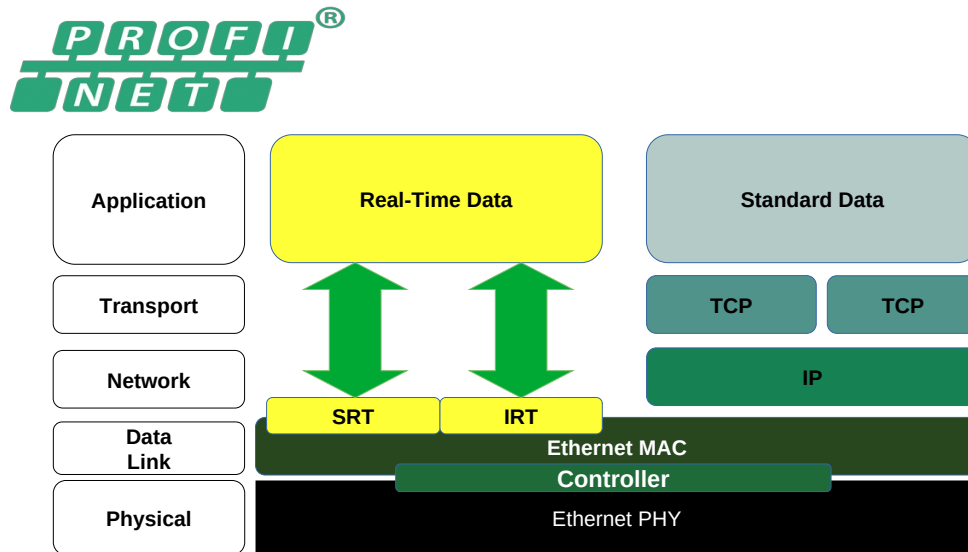


Figure 9: Profinet protocols

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.

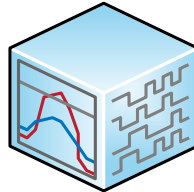
ProfiNet Soft-Real Time (SRT) handles the time-critical data exchange functioning in the way that when an SRT frame arrives in the destination node, the frame is directed from Layer 2, directly to the ProfiNet Layer 7, skipping the TCP/IP layers - thus improving the speed and determinism. The end performance 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.

4 Industrial Systems Scaling

4.1 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 10: 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.

4.2 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

4.3 OT Architecture

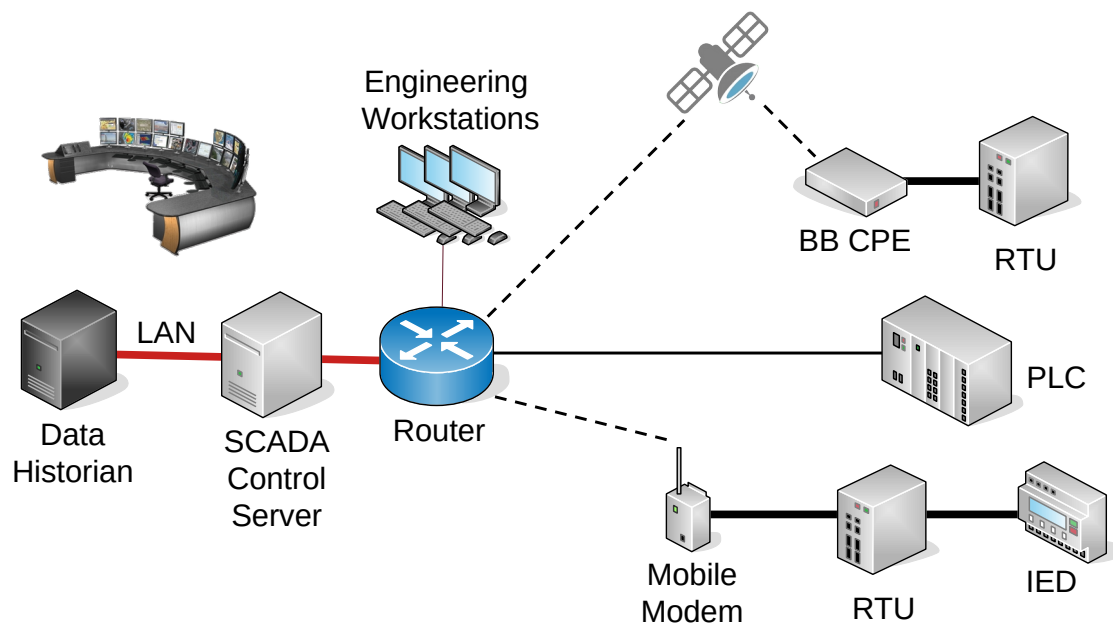


Figure 11: SCADA Architecture

Figure 11 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 Local Area Network (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 12: 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 RTU and/or PLCs, 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.

4.4 Distributed Control Systems

While SCADA is centralised, 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.

4.5 Safety Instrumented Systems



Figure 13: Fire Suppression System

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

4.6 Comparison SCADA/DCS/SIS

Table 2 provides a high-level comparison of SCADA, DCS, and SIS, highlighting their primary functions and characteristics.

Table 2: Comparison 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).

5 Physical Site Perimeter Defences

5.1 Physical Access Control Systems



Figure 14: 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.

5.2 Site and Facility Design

5.2.1 Location

The location of a facility is often decided on purely technical considerations; however, it is essential that security and environmental and safety concerns are also on the list of things that determine the final siting. Consider:

- Emergency Services
- Hazards and threats
- Agency to services.

5.2.2 Threats

Consider the site and facility design threat landscape. Devise a risk assessment and put controls in place to deal with each:

- Fire
- Water and flooding
- Storms
- Vandalism
- Sabotage
- Explosions
- Building failure, collapse
- Utility failure and continuity
- Equipment failures
- Access
- Strikes.

5.3 Secure Facility Plan & Physical Security Controls

The planning process should begin by involving all stakeholders and posing two fundamental questions:

- What is the threat, what is the organisation securing against?
- What levels of security are necessary and the organisation is willing to provide?

Once these questions are answered a list of possible threats should be drawn up.

The plan itself is developed using critical path analysis. With this process the company applications are systematically related with all the possible threats to it. A Database Server will require, hardware, software, power, temperature control. This leads to a critical look at the dependencies for this server, what if the electricity goes down, what if the hardware overheats.

5.4 Physical Access Controls

5.4.1 Fence

This is usually the first line of defence. The following guidelines should be considered when establishing such a fence.

- 1 metre Deter casual trespassers
- 2 metres Hard to climb easily
- 2.5 metres Delay determined intruders.

Another consideration is the planning laws in your locality. These may impact the type or look of the fence you plan.

A grass or gravel clearway along a fence should be considered to deter vehicles from parking near the fence. Bollards are a good method to deter such vehicles.

5.4.2 Access points

These points can be a weakness in the first layer of defence. By their nature gates provide access through the fence and therefore should be afforded the appropriate management.

5.4.3 Intrusion detection devices

- Photoelectric beams
- Ultrasonic
- Passive infrared
- Microwave
- Pressure sensitive pads

The use of intrusion detection systems can be mixed. They can either trigger audio or silent alarms or perhaps drown the area in light. One consideration however is the triggering of alarms by non intruders i.e. animals and birds.



Figure 15: Motion detector

5.4.4 Light

This is an very important consideration in your security plan. If it is dark it makes it easier for the intruder to access undetected. We also need to light areas to allow escape from the building in emergencies. Here are some of the lights that are typically encountered in an plant:

- **Continuous Lighting**
 - Fixed lights should be installed 2.5 metres above ground. The light on the ground from the lights should be at least 2 lumens.
- **Motion sensitive/trip lighting**
 - Sensor activated light can be both a good security deterrent and a cost effective alternative to continuous lighting.
- **Standby lighting**
 - Lights that come on in the event of power failure.
- **Exit lighting**
 - Lights to indicate the exit points.

5.4.5 Closed Circuit Television



Figure 16: CCTV

Closed Circuit Television (CCTV) is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors. CCTV equipment may be used to observe parts of a process from a central control room; when, for example, the environment is not suitable for humans.

CCTV systems may operate continuously or only as required to monitor a particular event.

A more advanced form of CCTV, utilising Digital Video Recorders (DVR) or Network Video Recorders (NVR), provides recording for possibly many years, with a variety of quality and performance options and extra features like motion-detection and email alerts.

Points to consider when installing CCTV systems:

1. The ability to **detect** an object
2. The ability to **recognise** a detected object
3. The ability to **identify** object details.

5.4.6 Security Guards

A security guard is a privately and formally employed person who is paid to protect property, assets, and people. Security officers are uniformed and act to protect property by maintaining a highly overt and visible presence to deter inappropriate access, observing for signs of crime, fire or disorder; then taking action and reporting any incidents to their client and emergency services as appropriate.

Generally the Security Guard will practice the *detect, deter, observe and report* methodology and call on the Gardaí or police when a situation is getting beyond their control.

Security officer's primary duty is the prevention and deterrence of crime. Security personnel enforce company rules and can act to protect lives and property. In fact, they frequently have a contractual obligation to provide these actions.

Security personnel may also perform access control at building entrances and vehicle gates, meaning, they ensure that employees and visitors display proper passes or identification before entering the facility. Security officers are often called upon to respond to minor emergencies (lost persons, lockouts, dead vehicle batteries, etc.) and to assist in serious emergencies by guiding emergency responders to the scene of the incident, helping to redirect foot traffic to safe locations, and by documenting what happened on an incident report.

5.4.7 Access Logs

Company:

Date:

Name	Company	Name of person visiting	Security Guard	Time in	Time out

Table 3: Access Log

Access logs should be maintained either in paper form though more commonly in electronic form to record the comings and goings on non employees.

5.5 Perimeter Security

5.5.1 Doors

1. Panels and glass should be protected against being kicked in or knocked out
2. Install metal lining on exterior wooden doors to resist drilling or sawing
3. Secure double doors with heavy duty, multiple-point, long flush bolts. Make sure the frame is as strong as the door
4. All exterior doors should be constructed of steel, aluminium alloy, or solid-core hardwood, with minimum 1.5mm steel on side and rear doors
5. Door frames should be securely fixed to the walls
6. Glass doors should have burglar-resistant glass installed
7. Doors should be secured with a minimum of 3 hinges
8. Doors should be clearly lit
9. Emergency doors should be clearly marked
10. Doors should provide entry and exit in the event of emergencies like power failure
11. Doors should have the same fire rating as the walls.

5.5.2 Locks

Exterior swinging doors should have a minimum 25mm deadbolt lock, 25mm throw bolt with a hardened insert, and free turning steel or brass tapered-cylinder guard. Steel strike plates should be used on aluminium door frames. All outside hinges should have non-removable hinge pins.

5.5.2.1 *Electronic/Electrical Locks*

An electronic or electric lock is a locking device which operates by means of electric current. Electric locks are sometimes stand-alone with an electronic control assembly mounted directly to the lock. More often electric locks are connected to an access control system. The advantages of an electric lock connected to an access control system include:

- Key control, where keys can be added and removed without re-keying the lock cylinder
- Fine access control, where time and place are factors
- Transaction logging, where activity is recorded

5.5.2.2 Authentication methods

Electronic locks offer a variety of means of authentication some are described below:

Numerical codes, passwords and passphrases

Perhaps the most prevalent form of electronic lock is that using a numerical code for authentication. The correct code must be entered in order for the lock to deactivate. Such locks typically provide a keypad. Combination lengths are usually between 4 and 6 digits long.

Security tokens

Another means of authenticating users is to require them to scan or swipe a security token such as a smart card or similar, or to interact a token with the lock.

Biometrics

As biometrics become more and more prominent as a recognised means of positive identification, their use in security systems increases. Some new electronic locks take advantage of technologies such as fingerprint scanning, retinal scanning and iris scanning, and voiceprint identification to authenticate users.

5.5.2.3 Padlocks

The most common assaults on padlocks are made with bolt cutters or crowbars. Quality padlocks should have the following features:

- Laminated or solid body case
- Hardened steel shackle with a minimum diameter of 8mm
- A double locking mechanism providing *heel and toe* locking, and at least 5-pin tumblers in the cylinder.

5.5.3 Turnstiles

A turnstile, also called a baffle gate, is a form of gate which allows one person to pass at a time. It can also be made so as to enforce one-way traffic of people, and in addition, it can restrict passage only to people who insert a security pass, or similar. Thus a turnstile can be used to restrict access to authorised people, for example in the lobby of an office building.



Figure 17: Turnstyle

From a security standpoint, they lead patrons to enter single-file, so security personnel have a clear view of each patron. This enables security to efficiently isolate potential trouble or to confiscate any prohibited materials. Thus, turnstiles are a tool which leads to a more safe and secure atmosphere throughout a site.

5.5.4 Mantrap

A mantrap refers to a small space having two sets of interlocking doors such that the first set of doors must close before the second set opens. ID may be required for each door, and possibly different measures for each door. For example, a key may open the first door, but a personal identification number entered on a number pad opens the second. Other methods of opening doors include proximity cards or biometric devices such as fingerprint readers or iris recognition scans.

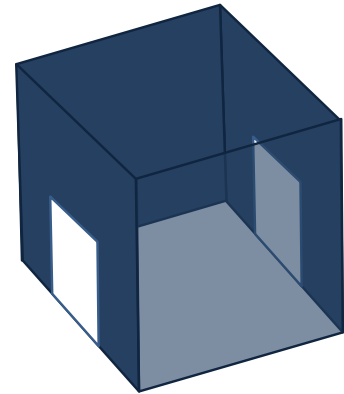


Figure 18: Mantrap

Mantraps may be configured so that when an alarm is activated, all doors lock and trap the suspect between the doors in the *dead-space* or lock just one door to deny access to a secure space.

5.5.5 Windows

Windows should offer light, ventilation, and visibility, but not easy access. Locks should be designed so they cannot be reached and opened by breaking the glass. First floor windows should be protected with burglar-resistant glass, bars, grilles, grates, or heavy-duty wire screening to provide optimum window security.

5.5.5.1 Plate Glass

This is the most common type of glass found in windows. It is easy to get and cut for openings and for replacement. One problem is it tends to shatter in shards when broken or subject to an explosion. This presents a safety hazard.

5.5.5.2 Tempered Glass

This form of glass has been processed by controlled thermal or chemical treatments to increase its strength compared with normal glass. Tempered glass is made by processes which create balanced internal stresses which give the glass strength. It will usually shatter into small fragments instead of sharp shards when broken, making it less likely to cause severe injury and deep lacerations.

5.5.5.3 Polycarbonate Glass

This is not really glass but thermoplastic polymer moulded to look like glass. Fabrication is done with fine tooth saws. Polycarbonate is the toughest glazing available for windows. It very difficult to cut with a knife, but it is easily scratched, damaging the appearance.

6 Environmental Constraints

6.1 Power

The maintenance of a secure and sustained power source is essential for technology businesses, data centres and technical laboratories.

Power problem terms

- **Fault** – This is a momentary loss of power
- **Blackout** – Complete loss of power
- **Sag** – Lowering of the power supply voltage
- **Brownout** – Prolonged period of low voltage
- **Spike** – Momentary increase in voltage
- **Surge** – Prolonged period of high voltage
- **Noise** – A continuous power fluctuation
- **Transient** – A short period of noise
- **Ground** – Electrical earth
- **Clean** – Continuous non fluctuating power
- **Inrush** – Surge of voltage given initially after a device is connected to a power source.

6.1.1 Uninterruptible Power Supply

A Uninterruptible Power Supply (UPS) or sometimes called a battery backup, is an electrical device that provides emergency power when the input power source, typically the mains, fails. A UPS differs from an auxiliary or emergency power system or standby generator in that it will provide instantaneous or near-instantaneous protection from input power interruptions by means of one or more attached batteries and associated electronic circuitry. The on-battery runtime of most uninterruptible power sources is relatively short 5 – 15 minutes being typical for smaller units but sufficient to allow time to bring an auxiliary power source on line, or to properly shut down the protected equipment.

6.1.2 Electrical/Electronic Noise

In electronics and communication systems, noise is a random fluctuation or variation of an electromagnetic analogue signal such as a voltage or a current. Electronic noise is a characteristic of all electronic circuits. Depending on the circuit, the noise generated by electronic devices can vary greatly. Noise can be produced by several different effects. Thermal noise and shot noise are inherent to all devices. The other types depend mostly on manufacturing quality and semiconductor defects.

6.2 Water and Fire

6.2.1 Development of a Fire

A fire develops typically in four stages, and fire detectors are designed to detect some characteristic effect of one or more of these stages:

- **Incipient stage**
 - No visible smoke, no flame and very little heat
 - A significant amount of invisible (but sometimes detectable by smell) combustion particles may be created
 - This stage usually develops slowly.
- **Smouldering/smoke stage**
 - Smoke, but no flame and little heat.
- **Flame stage**
 - Visible flame, more heat, often less or no smoke, particularly with flammable liquids and gas fires.
- **Heat stage**
 - Large amounts of heat, flame, smoke and toxic gases are produced.
 - The transition from the previous stage can be very fast.

6.2.2 Fire triangle

The fire triangle is a simple model for understanding the ingredients necessary for most fires.

The triangle illustrates the rule that in order to ignite and burn, a fire requires three elements: heat, fuel, and an oxidising agent (usually oxygen). The fire is prevented or extinguished by removing any one of them. A fire naturally occurs when the elements are combined in the right mixture.

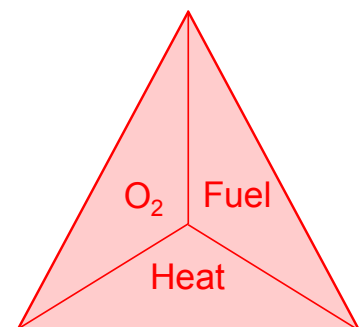


Figure 19: Fire triangle

Without sufficient heat, a fire cannot begin, and it cannot continue. Without fuel, a fire will stop. Without sufficient oxygen, a fire cannot begin, and it cannot continue.

6.2.3 Fire Classes

European	American	Fuel/Heat source	Agents
Class A	Class A	Ordinary combustibles	Water
Class B	Class B	Flammable liquids	CO ₂ , Foam
Class C		Flammable gases	Dry chemical, Gas
Class D	Class D	Combustible metals	Dry Powders
Class E	Class C	Electrical equipment	CO ₂ , Foam, Gas
Class F	Class K	Cooking oil or fat	Wet chemical



Figure 20: Fire Classes

Fires are identified according to one or more fire classes. Each class designates the fuel involved in the fire, and thus the most appropriate extinguishing agent. The classifications allow selection of extinguishing agents along lines of effectiveness at putting the type of fire out, as well as avoiding unwanted side effects.

6.2.4 Fire management in OT

With all the electronics in utilities and manufacturing OT, fire is a real risk. Typically water is used in fire control but used on electronic equipment will result in further damage to the equipment. For this reason Halon 1301 Gas was used in such environments. Unlike water, Halon 1301 didn't damage equipment however it did damage the ozone layer. The Montreal Protocol of 1987, limited the production of Halon 1301 to roles like aircraft emergency equipment where another alternative did not exist.

Halon 1301 was replaced by a number of extinguishing agents like Argon and Inergen when protecting data centres. They fall into two broad categories:

- **Halocarbon gases**
 - These work by removing heat from the fire
 - The room must be evacuated before the release of these agents
 - Lower storage space requirement compared to inert gases
 - Fast fire suppression time (10sec)
 - Must be very near point of use (max 30m)
 - More expensive than inert gases.
- **Inert gases**
 - These suppress fires by lowering the oxygen concentration in the room below the level needed to sustain combustion
 - Perform more effectively in rooms that aren't well sealed
 - More gas required than Halocarbon gases to suppress an area
 - These can be piped long distances (100 – 200m) to a room and still retain their effectiveness.

6.2.5 Pre-action Sprinklers

Pre-action sprinkler systems also are an option. The best choice for a particular facility will depend on the system's overall cost, the way in which the system will be used and the space available to house the extinguishing substance. The pipes in pre-action sprinkler systems do not hold water which reduces the risk of leaks that could damage computer or telecommunications equipment.

Instead, a valve within the system is located outside the data centre and keeps water from entering. In order for water to get past the valve, a smoke detector has to let the system know that a fire is occurring; at that point, water moves into the pipes. However, the fire has to grow to a certain temperature before the valve will open and water can discharge into the room. Given that these two events have to occur before water will flow through the pipes that are located within the data centre, the risk of an accidental leak is greatly reduced.

6.3 Water threat

Water damage is a threat in itself. Information systems and paper records can be badly damaged should they get wet particularly if saturated. Data centres and laboratories should be considered for water detection sensors that can trigger an alarm. Such rooms having raised floors to allow time for a water threat to be reacted to are common (though these are also used for conduits to carry room power and network cabling. Water threats are another reason to place such rooms above ground level.

6.4 Heating, Ventilating, and Air Conditioning

HVAC is the technology of indoor environmental comfort plus temperature and humidity control in data centres and laboratories. HVAC is particularly important in the design of medium to large industrial and office buildings such as skyscrapers and in marine environments such as aquariums, where safe and healthy building conditions are regulated with temperature and humidity, as well as *fresh air* from outdoors.

6.4.1 Positive Pressure

By applying greater air pressure in the room or building than is outside which ensures that should there be any leakage it will be out and thus prevent any unwanted air in. Monitoring of air pressure in a controlled room is a method that can be applied to the alarm system. Should the pressure change suddenly it is an indication of the possibility of unauthorised access.

7 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*, International Standard IEC 61784-1-1:2023, Mar. 22, 2023.
- [3] IEC 61158, *Industrial networks - Profiles - Part 1-0: Fieldbus profiles - General concepts and terminology*, International Standard IEC 61158-1:2023, Mar. 16, 2023.

This page is intentionally blank