Topic 1

Introduction and Operational Technology Overview

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:

- Key terms in Cybersecurity
- Define Operational Technology (OT)
- Define Critical Infrastructure in terms of the Network Information Systems (NIS)
- Explain the Critical Evolutions in OT
- Consider the Security Implications of OT
- List the differences between Information Technology (IT) and OT
- Explain the CIA Triad and the need to invert it for OT Security (OTSec).

2 Introduction

As manufacturing becomes more automated, digitised and network-enabled, the risks and attack surfaces increase. OT deployment and usage is expanding and cybersecurity professionals need to be more aware of the area and the implications for security. This topic explores the fundamental concepts of industry best practice for cybersecurity within OT environments helping with the understanding of how OT supports critical infrastructure and therefore the global requirement for OT security, as it proliferates across various industries. Staff and public safety are the first concern when working within an industrial setting. This priority also extends to cybersecurity incident response.

3 IT versus OT

3.1 Information Technology

Any equipment or interconnected system used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an organisation or by a 3rd party on the organisations behalf.

IT includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

3.2 Operational Technology

Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include Industrial, Automation and Control Systems, Building Management Systems (BMS), Fire Control Systems (FCS), and Physical Access Control mechanisms.

4 Cybersecurity terms and Concepts

Figure 1: Risk example

4.1 Asset

In almost any context, an asset is a positive thing, and it often has worth. Money is an asset, for example. When you list assets and liabilities, assets are all things that have value. In broad terms, an asset can be people, property, or information. But it can also include your online reputation or a database of customer information. A machine within an industrial setting is also an asset. Anything that has a value to the owner and needs to be protected is an asset.

4.2 Threat

Any circumstance or event with the potential to adversely impact organisational operations (including mission, functions, image, or reputation), organisational assets, individuals, other organisations, or the nation through an information system via unauthorised access, destruction, disclosure, modification of information, and/or Denial of Service (DoS).

4.3 Vulnerability

The only way a threat can do damage to an asset is if the asset has an unchecked vulnerability that the threat can take advantage of. In the house example, a vulnerability could be a security system that relies on electricity. If there is no battery backup, the burglar could take down the power and then have free access to the home. Another vulnerability could be something as simple as an unlocked window. Anything that a burglar could take advantage of is a vulnerability.

By that same token, in an industrial setting a Programmable Logic Controller (PLC) can have vulnerabilities that hackers can take advantage of. Legacy PLC's that are not updated or maintained can be as dangerous as they can an access to a facility, equipment or service. If firmware is not updated regularly, then vulnerabilities can be made available for hackers to gain access. Put all of this together, and there is risk.

5 Risk

Risk is the potential for loss, damage or destruction of an **asset** as a result of a **threat** exploiting a **vulnerability.** Risk is a function of threats taking advantage of vulnerabilities to steal or damage assets. Understanding these separate concepts helps to understand how safe an industrial environment really is. Threats, like hackers, may exist. But if there are no vulnerabilities within the people, processes or technology of the environment, then risk is very low. Vulnerabilities may exist in the environment, but if threats do not exist, then there is still little risk (this is not really an option, however, as hackers are very prevalent online). For industrial cybersecurity, the goal is to close off any vulnerabilities so that assets remain safe.

5.1 Risk Management

From the point of view of risk management there are a number of ways in which risks can be treated, these include:

Risk Acceptance

- Management deem the risk acceptable, compared to the cost of implementing controls to mitigate against it.

Risk Mitigation

- Implement a suitable control or combination of controls to reduce (mitigate) the risk to an acceptable level.

Risk Avoidance

- Avoiding the risk all together making a decision not to enter into the associated activity.

Risk Transfer

- Transfer the risk to another organisation. For example, purchasing of insurance for equipment.

5.2 Risk Appetite

The level of risk that an organisation is prepared to accept in pursuit of its objectives, before action is deemed necessary to reduce the risk. It represents a balance between the potential benefits of innovation and the threats that may affect the organisation achieving its objectives.

5.3 Mitigating Controls

Where a risk assessment identifies a risk, which the risk owner cannot treat fully for some reason (resources, time, budget). The risk owner may decide to reduce the risk to an acceptable level by putting in place mitigating controls, which do not fully remove the risk but will lower the likelihood of it occurring.

5.4 Residual Risk

This is the level of risk remaining when a risk treatment was implemented; typically, it is lower than the initial risk level due to the introduction of the risk treatment control.

5.5 Risk Assessment

A cyber security risk assessment identifies the industrial assets that could be affected by a cyber attack (such as hardware, systems, PLC, communication protocols). It then identifies the risks that could affect those assets. Risk estimation and evaluation are usually performed, followed by the selection of controls to treat the identified risks. When performing risk the availability, integrity and confidentiality of the system are considered. A method of comparing the severity of risk is usually defined in a risk management policy. When determining the severity of risk quite often a matrix similar to that illustrated in Figure 2 is used. This considers the likelihood of a risk happening with the impact of the risk should it occur. In this manner individual risks are given a score ranging between 0 and 8. In this example any risk scoring above a value of 6 (red zone) will require treatment by adding appropriate controls. It is essential to continually monitor and review the risk environment to detect any changes in the context of the organisation, and to maintain an overview of the complete risk management process.

	Likelihood				
Impact	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Description	Value Range
Insignificant Risk	0 - 2
Acceptable Risk	3 - 5
Unacceptable Risk	6+

Figure 2: Risk Matrix

5.6 Risk Registers

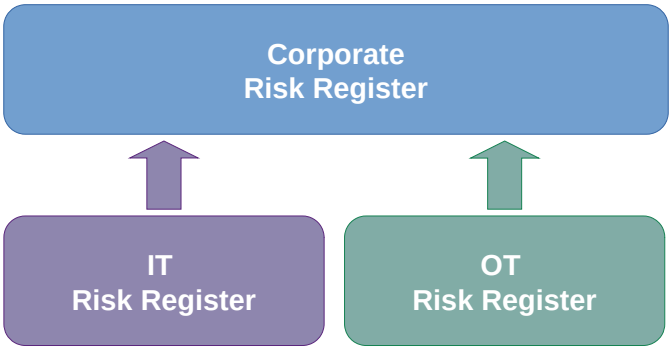

Figure 3: Risk Registers

The Corporate Risk Register contains details of all of the risks to the organisation. It is a tool that captures, describes and assesses risks as they are identified, together with risk accountabilities, actions where required, review dates and dates when actions were completed and the risk item closed. It will include the date of the last assessment, a description of the risk, an estimate of the impact and the likelihood, any mitigating controls, and a statement of action required, with target date and owner. A properly maintained risk register provides a useful vehicle for communication.

The IT Risk Register records the risks identified with Information Communications Technology (ICT) and Information Systems (IS).

The OT Risk Register similarly records risk identified within the industrial zone of the organisation.

While many companies will bundle this into the Corporate Risk Register, larger organisations tend to have one Register per department with the highest severity risks being promoted to the Corporate Risk Register.

These Risk Registers are owned by the Senior Management Team (SMT) since the acceptance of risks contained therein is not the responsibility of ICT, given that some of the risks will affect business areas.

5.7 AAA Framework

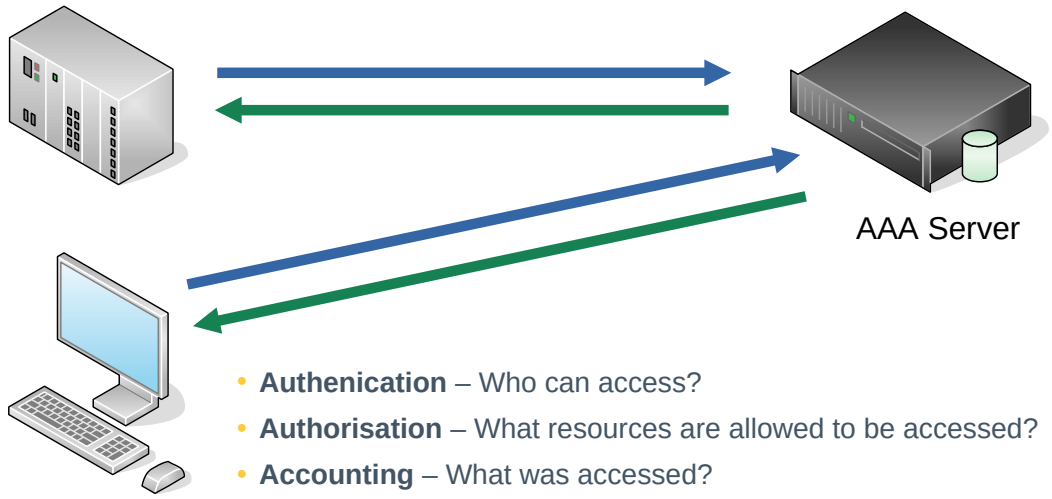

Figure 4: AAA Framework

Authentication, Authorisation, and Accounting (AAA) framework is the logic behind Identity Management systems.

5.7.1 Authentication

Authentication is the act of confirming the truth of an attribute of a single piece of data claimed true by an entity. In contrast with identification, which refers to the act of stating or otherwise indicating a claim purportedly attesting to a person or thing's identity, authentication is the process of actually confirming that identity. There are four primary types of authentication.

They use:

- **Static passwords**
- **One Time Password (OTP)** such as Personal Identification Numbers (PIN) delivered through Short Messaging Service (SMS) texts or push notifications
- **Digital certificates** (x.509 digital certificate)
- **Biometric credential** (Fingerprint, Facial recognition, etc...)

Additionally, there are three categories:

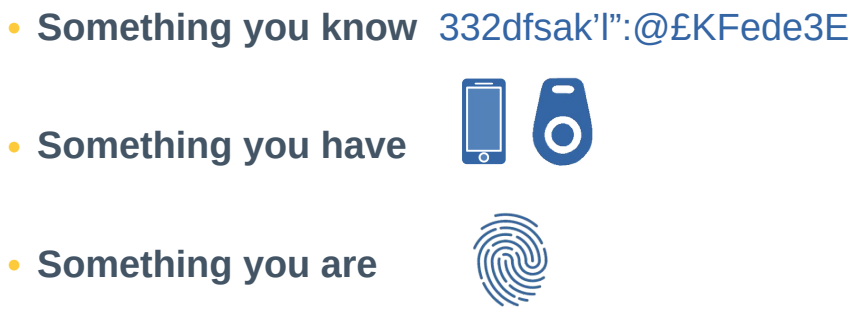

Figure 5: Something you .....

When more reliable Authentication is required, a Multi-Factor Authentication (MFA) is employed which makes it difficult for someone to authenticate as another person. For example, if a thief steals a mobile phone, he would also have to obtain the user's password to access the code sent by an SMS text or possess the key fob that displays the code. Using two passwords is not considered MFA because both passwords are considered "something you know". Many companies are moving toward MFA or Two-Factor Authentication (2FA) which leverages a static password and OTP or challenge question to strengthen security. Biometric authentication is being adopted as well.

5.7.2 Authorisation

Authorisation is the function of specifying access rights/privileges to resources related to information security and computer security in general and to access control in particular.

After a user identifies himself and is authenticated to prove his identity, he must pass the authorisation rule to access system services, programs and data. Authorisation determines what the user can access and what he cannot access. An important concept to understand is the following: a user may authenticate but the resultant authorisation could still be DENY ACCESS.

The Principle of Least Privilege requires that users and devices must only be granted sufficient access necessary to perform their required functions. Any frivolous authorisation can result in accidental or malicious violations of security policy.

5.7.3 Accounting

This is the process that keeps track of a user's activity while attached to a system; the trail included the duration of time attached, the resources accessed, and the volume of data transferred. Accounting data is used for trending, detecting breaches, and forensic investigating. Keeping track of users and their activities serves many purposes. For example, tracing back to events leading up to a cybersecurity incident can prove very valuable to a forensics analysis and investigation case.

6 Reverse Proxy

A reverse proxy is a server that sits in front of web servers and forwards client (e.g. web browser) requests to those web servers. Reverse proxies are typically implemented to help increase security, performance, and reliability. In order to better understand how a reverse proxy works and the benefits it can provide, let's first define what a proxy server is.

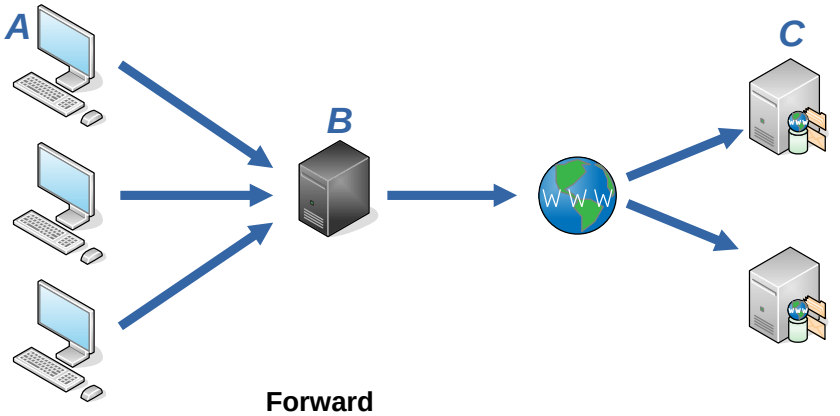

Figure 6: Proxy Server

6.1.1 What's a proxy server?

As illustrated in Figure 6, forward proxy, often called a proxy, proxy server, or web proxy, is a server that sits in front of a group of client machines. When those computers make requests to sites and services on the Internet, the proxy server intercepts those requests and then communicates with web servers on behalf of those clients, like a middleman. For example, name 3 computers involved in a typical forward proxy communication:

- A: This is a user's home computer
- B: Forward proxy server
- C: This is a website's origin server (where the website data is stored)

In a standard Internet communication, computer A reaches out directly to the server C, with the client sending requests to the origin server and the origin server responding to the client computer A. When a forward proxy is in place, computer A will instead send requests to the proxy B, which will then forward the request to server C. Server C will then send a response to the proxy B, which in turn will forward the response back to computer A.

Why would anyone add this extra middleman to their Internet activity? There are a few reasons one might want to use a forward proxy:

- **To avoid state or institutional browsing restrictions** - Some governments, schools, and other organisations use firewalls to give their users access to a limited version of the Internet. A forward proxy can be used to get around these restrictions, as they let the user connect to the proxy rather than directly to the sites they are visiting.
- **To block access to certain content** - Conversely, proxies can also be set up to block a group of users from accessing certain sites. For example, a school network might be configured to connect to the web through a proxy which enables content filtering rules, refusing to forward responses from Facebook and other social media sites.
- **To protect their identity online** - In some cases, regular Internet users simply desire increased anonymity online, but in other cases, Internet users live in places where the government can impose serious consequences to political dissidents. Criticising the government in a web forum or on social media can lead to fines or imprisonment for these users. If one of these dissidents uses a forward proxy to connect to a website where they post politically sensitive comments, the IP address used to post the comments will be harder to trace back to the dissident. Only the IP address of the proxy server will be visible.

6.1.2 How is a reverse proxy different?

A reverse proxy is a server that sits in front of one or more web servers, intercepting requests from clients. This is different from a forward proxy, where the proxy sits in front of the clients. With a reverse proxy, when clients send requests to the origin server of a website, those requests are intercepted at the network edge by the reverse proxy server. The reverse proxy server will then send requests to and receive responses from the origin server.

The difference between a forward and reverse proxy is subtle but important. A simplified way to sum it up would be to say that a forward proxy sits in front of a client and ensures that no origin server ever communicates directly with that specific client. On the other hand, a reverse proxy sits in front of an origin server and ensures that no client ever communicates directly with that origin server.

Consider illustration Figure 7 where the following devices are identified as:

- D: Users’ home computers
- E: Reverse proxy server
- F: One or more origin servers

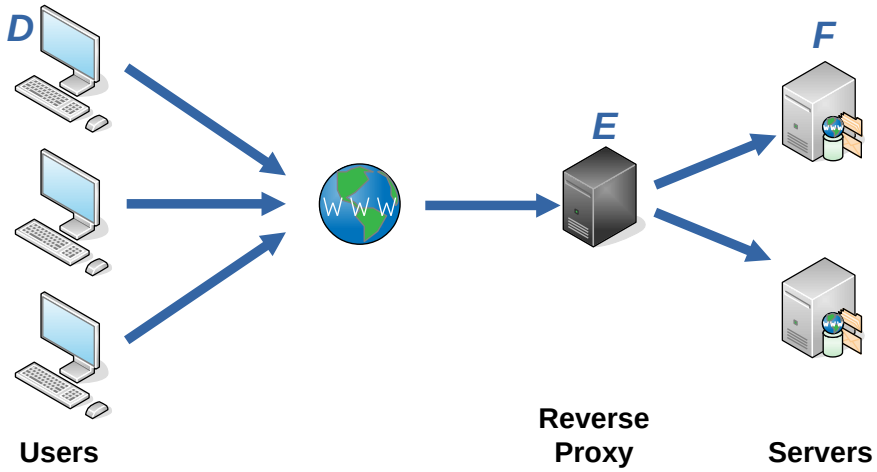

Figure 7: Reverse Proxy

Typically all requests from computer D would go directly to server F, and server F would send responses directly to computer D. With a reverse proxy, all requests from computer D will go directly to reverse proxy E, and reverse proxy E will send its requests to and receive responses from server F. Reverse proxy E will then pass along the appropriate responses to computer D.

Below is outlined some of the benefits of a reverse proxy:

- **Load balancing** - A popular website that gets millions of users every day may not be able to handle all of its incoming site traffic with a single origin server. Instead, the site can be distributed among a pool of different servers, all handling requests for the same site. In this case, a reverse proxy can provide a load balancing solution which will distribute the incoming traffic evenly among the different servers to prevent any single server from becoming overloaded. In the event that a server fails completely, other servers can step up to handle the traffic.
- **Protection from attacks** - With a reverse proxy in place, a web site or service never needs to reveal the IP address of their origin server(s). This makes it much harder for attackers to leverage a targeted attack against them, such as a DDoS attack. Instead the attackers will only be able to target the reverse proxy, such as Cloudflare's Content Deliver Network (CDN), which will have tighter security and more resources to fend off a cyber attack.
- **Global Server Load Balancing (GSLB)** - In this form of load balancing, a website can be distributed on several servers around the globe and the reverse proxy will send clients to the server that's geographically closest to them. This decreases the distances that requests and responses need to travel, minimising load times.
- **Caching** - A reverse proxy can also cache content, resulting in faster performance. For example, if a user in Paris visits a reverse-proxied website with web servers in Los Angeles, the user might actually connect to a local reverse proxy server in Paris, which will then have to communicate with an origin server in L.A. The proxy server can then cache (or temporarily save) the response data. Subsequent Parisian users who browse the site will then get

the locally cached version from the Parisian reverse proxy server, resulting in much faster performance.

- **Secure Sockets Layer (SSL) encryption** - Encrypting and decrypting SSL (or Transport Layer Security (TLS)) communications for each client can be computationally expensive for an origin server. A reverse proxy can be configured to decrypt all incoming requests and encrypt all outgoing responses, freeing up valuable resources on the origin server.

7 Introduction to Operational Technology

When one considers the inside a modern factory, distribution centre, or any other industrial environment, it is impossible not to notice the vast array of different types of equipment, such as conveyor belts, forklifts, packaging machines, and everything else necessary to assemble a set of components into a finished product or move packages through a supply chain, or keep a guest pipeline in operation.

Today, just about everything that can be seen is in some way connected to some form of network. Both networks that use an industrial protocol or a common Ethernet network. Everything that's connected to one of those networks is there because it's providing information or controlling something. For example, a temperature sensor or a flow control valve, or even a component of a machine for sorting out widgets as they move along a production line. In turn, those sensors and controllers have software interfaces so that they can be programmed. Software interfaces are installed onto different types of computers, so their operators have an interface that they can use to perform the controlling and monitoring activities. All of these things together make up an Industrial Control System (ICS).

In some standards this is broadened to encompass Automation as Industrial Automation and Control Systems (IACS). To differentiate between the two, IACS can be defined as a collection of personnel, hardware, software and policies that “controls” the industrial process and can affect or influence its safety, security and its reliable operation, it means, anything that interacts and could affect the system, it belongs to the IACS system.

Operational Technology (OT) is another term that is used, this encompasses the computing systems that manage industrial operations, including the Electrical, Gas, Water, Telecommunications utilities as well as manufacturing operations, and more. OT runs the networks that allow critical utilities to operate. SO essentially OT is a broad term for ICS and IACS.

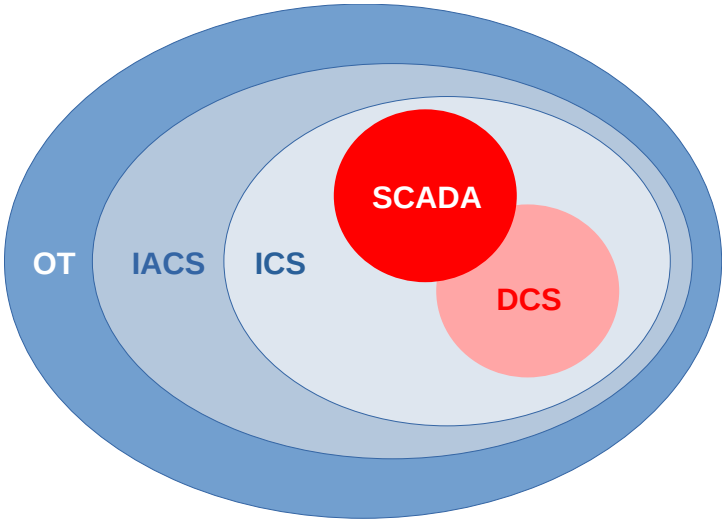

Figure 8: OT -v- IACS -v- ICS

8 Operational Technology

There are many and varied aspects to OT environments. As a cybersecurity practitioner, it is necessary to have a good understanding of these differences so that the correct key concepts, concerns and questions are applied in each situation.

First, consider the implications for OT within an Electrical power generation station. The Electrical industry, across many countries, is classified as Critical National Infrastructure (CNI). As critical infrastructure, it supplies power to homes and industries across the country. The key elements to consider when exploring the generation station. Operational Technology are:

- The size of such facilities and the concerns for operations and security.
- Balancing the IT perspective and the OT perspective.
- The paramount importance of safety concerns for health and human life.

As an alternative, and quite different OT environment consider the prospect of establishing a new factory to manufacture a breakthrough healthcare imaging device. Healthcare is an immensely complex industry and this scenario will only begin to address one aspect of the OT implications.

Other OT environments again can be found within the food industry, there are different types of facilities. From food processing facilities as well as food manufacturers. While the food industry may not be classified as critical infrastructure, however, due to the nature of the product, there are significant safety concerns. Food processing facilities are often smaller than some of their counterparts such as the Electrical generation. Like other OT environments, there is often a hybrid mixture of legacy Supervisory Control And Data Acquisition (SCADA) systems with automated systems.

9 Critical Infrastructure Sectors

Most countries define and specify their critical infrastructures and often group them into sectors. In terms of actual industrial control systems, one major factor that determines how systems are architected and secured is regulation.

9.1 Critical Infrastructure

The EU, the UK and the US group and define critical infrastructure sectors differently; however, all three contain the same facilities, just defined differently.

9.1.1 In the EU

The EU Network Information Systems version 2 (NIS2) [1] and Resilience of Critical Entities [2] directives group sectors of high criticality as:

- Energy
  - *Electricity*
  - *District heating and cooling*
  - *Oil*
  - *Gas*
  - *Hydrogen*
- Transport
  - *Air*
  - *Rail*
  - *Water*
  - *Road*
- Banking
- Financial market infrastructures
- Health
- Drinking water
- Waste water
- Digital infrastructure
- ICT service management (business-to-business)
- Public administration
- Space

Figure 9 is an example of a Critical Entity, it is an Electricity Supply Board (ESB) gas-powered electrical generation station that supplies electricity to Cork City, Ireland.

Further to these high critical sectors there are other critical sectors defined as follows:

- Postal and courier services
- Waste management
- Manufacture, production and distribution of chemicals
- Production, processing and distribution of food
- Manufacturing
- Digital providers
- Research

Figure 9: ESB Agsada gas fired Power Station, Cork, Ireland

9.1.2 In the UK

The UK Cabinet Office has, through the National Protective Security Authority (NPSA), defined 13 National Infrastructure sectors [3]. Several sectors have defined sub-sectors; Emergency Services for example can be split into Police, Ambulance, Fire Services and Coast Guard. The sectors are:

- Chemicals
- Civil Nuclear Communications
- Defence
- Emergency Services
- Energy
- Finance
- Food
- Government
- Health
- Space
- Transport
- Water

10 Critical Evolutions in OT

10.1 Industrial Revolution

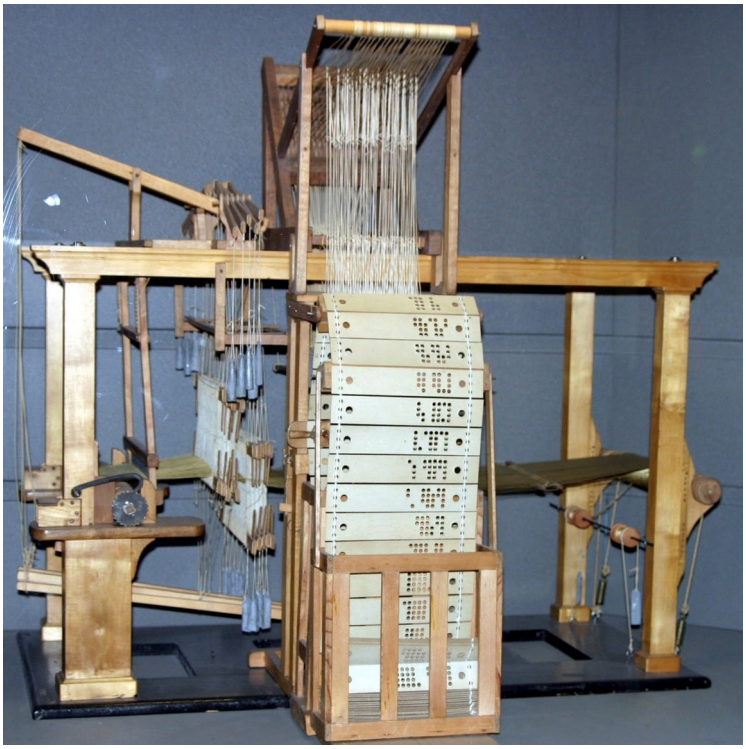

Figure 10: From loom to computer

The increase in complexity of industrial automation over the past century has seen greater efficiencies and the production of utilities and products at lower costs. Looking back there are a many examples of the introduction of automation, for example the introduction of punchcards readers in textile looms, in the North of England in the mid 1800s, led to the automation of pattern weaving thereby reducing labour costs and increasing output.

10.2 Early Age of Computing

Ada Lovelace took the idea and applied it to write programs for Charles Babbage's Analytical engine [4]. More recent examples include the use of gyroscopes that were designed for aircraft autopilots during the first decade of the 20th century. The biggest advances in early control system technology occurred during the pre-World War II period and actually during the war itself. This was to solve problems associated with things like tracking targets and platform stability. Consider aircraft bomb aimers looking at a bomb sight, these were stabilised control systems.

10.3 Computing after World War 1

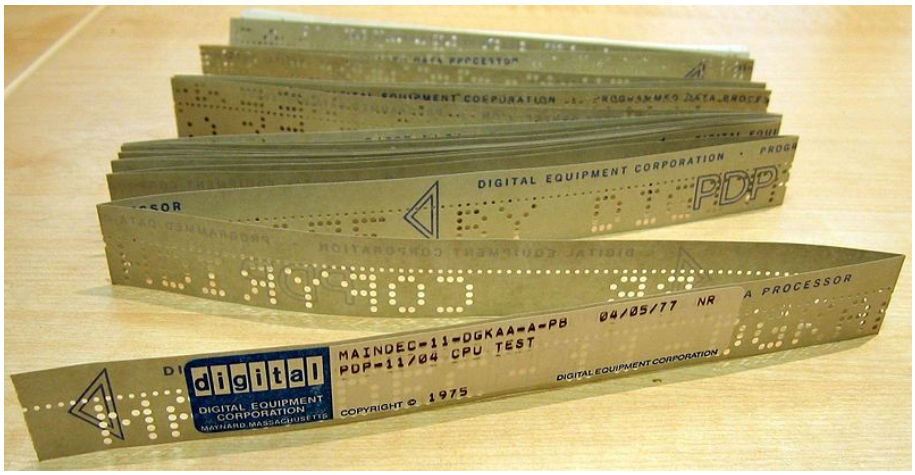

Figure 11: 1950s: Computer paper tape used to store programs

The computer control systems that we know today are very closely linked to the invention of the first data processing machines, the precursor to modern computers. The punch tape that Ada Lovelace made use of in the mid-1800s was still in use with mainframes in the 1950s with COmmon Business-Oriented Language (COBOL) software.

10.4 Computing and Industrial Control

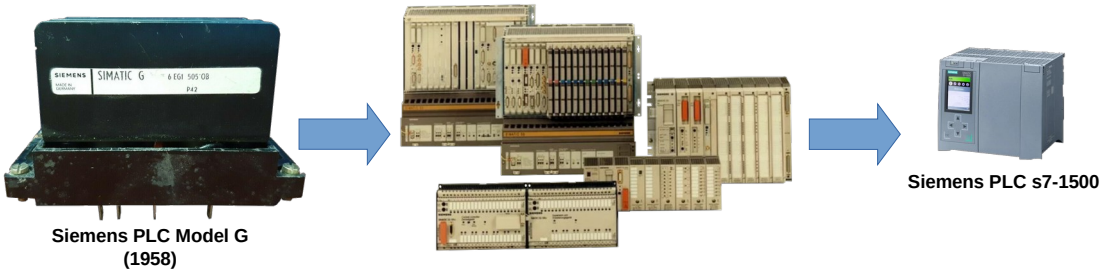

Figure 12: Siemens PLCs from 1958 to today

PLC, first came into play in the 1960s within the car manufacturing industry to manage the frequent changes in the configuration of the machines that were used on the production lines. The main problem with them was that factory floor workers needed to learn computer programming, sometimes in low-level languages such as assembler, to operate and troubleshoot them. However, when it was first realised that many of the factory electricians were familiar with ladder logic, changes were made to the way that PLCs were developed to make them easier to program, and ladder logic became the principal means of programming a PLC, as it is today. The first modern PLCs were made during the late 1960s, and they began to be widely deployed by electrical and gas utility and pipeline companies, and in turn leading to the development of SCADA systems for controlling and monitoring PLCs over a large geographic area.

11 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.

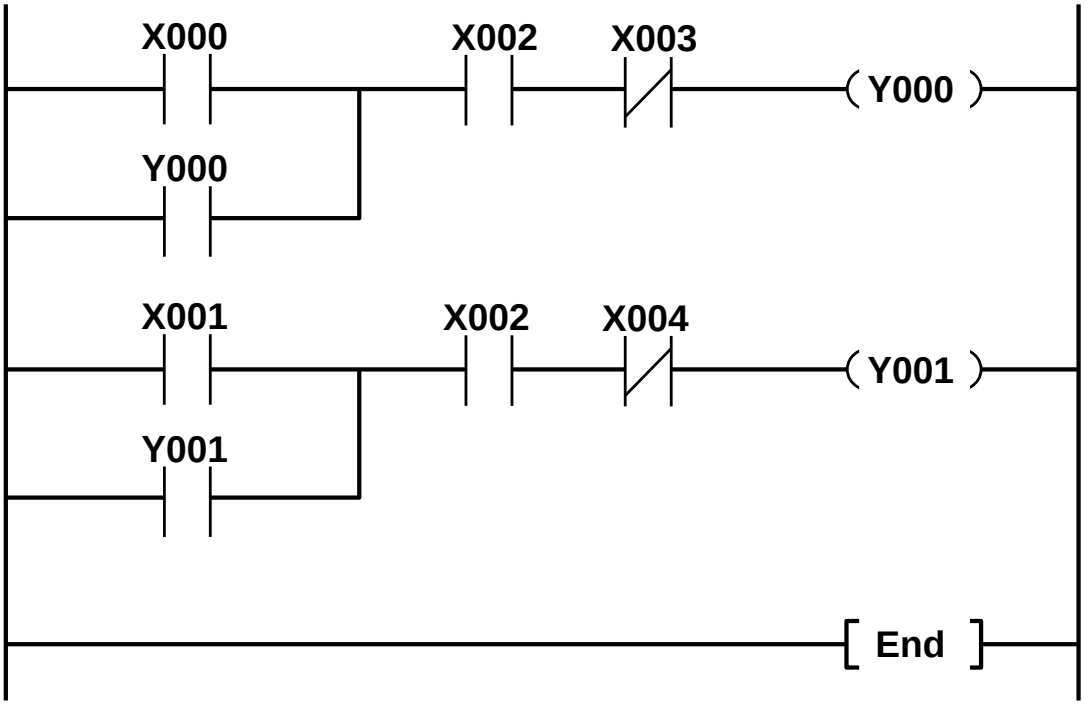

Figure 13: Ladder Logic

12 Evolution of Operational Technology

OT has continued to evolve as IT capabilities are inserted into existing physical systems. In many cases these replace or supplement physical control mechanisms. This evolution has been encouraged through the improvements in both cost and performance and this has lead to the “smart” technologies we have today.

Figure 14: ESB "Smart" meter

For example the electricity meters in homes across Ireland have been replaced with “smart” meters. These “smart” meters benefit the ESB as they give accurate real-time readings and are more difficult to tamper with. The consumer benefits too as “smart” meters measures electricity usage without the need for estimated meter readings and they will only reflect the electricity actually used. The consumer no longer have to submit readings or have someone read the meter. These meters also provide the consumer with greater access to accurate information on energy usage,and therefore the consumer has greater control over their energy consumption. By changing behaviour based on more insightful insights, the consumer can reduce bills as well as their carbon footprint.

Engineering models and analysis are evolving to address these emergent properties, including safety, security, privacy, and environmental impact interdependencies.

13 Consideration of Security Implications

Consider the security implications of having a network that has legacy systems, such as Windows XP, connected to it. It's not just workstations and server systems to consider but also old network infrastructures such as switches, routers and firewalls.

14 IT and OT

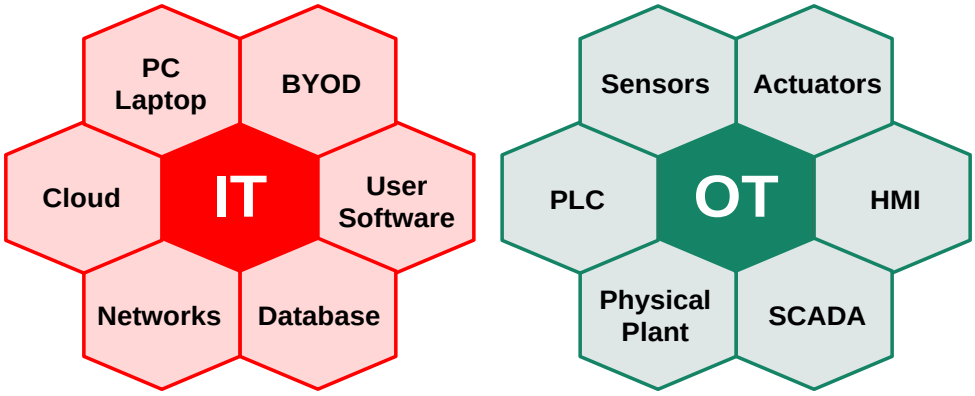

Figure 15: IT -v- OT

The purpose of OT is to use a computer to control some machine and perform a mechanical task. For example, opening a valve or controlling a temperature. Because OT systems can be used to monitor industrial systems, such as the control components of a production line, or valves in an oil pipeline, they need to be very reliable with a high rate of availability. An IT system is generally more for processing and storing information, and executing the software that businesses use. Now, of course, an IT system may also need to be highly available and reliable. But the software it runs does not directly affect a physical object. Consider when you press the enter button, it could be for a task such as saving some data to a file or a database, rather than making an actuator move a robotic arm on a production line. That's not to say that an IT system ca not control their device, we know that they can, but in this case and within an industrial setting, that computer has now become OT.

Is there a conflict between OT and IT? For example between those who manage OT systems and those who manage IT systems. This can happen, and examples where IT departments have attempted to deploy software onto OT computers without having a complete awareness of how the OT system is used is common enough. This can lead to problems with production. It is far better if there is a working relationship developed between IT and OT staff who can work together towards the same objective, which is keep production running.

Although some characteristics are similar, OT has unique performance and reliability requirements and often use OSs and applications that may be considered unconventional to typical IT personnel. Furthermore, the goals of safety and efficiency sometimes conflict with security in the design and operation of OT systems.

Threats to OT systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, malicious intruders, complexities, accidents, and natural disasters as well as malicious actions by insiders. OT security objectives typically follow the priority of integrity and availability, followed by confidentiality.

Possible incidents an OT system may face include [5]:

- Blocked or delayed flow of information through OT networks, which could disrupt OT operation.
- Unauthorised changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment, create environmental impacts, and/or endanger human life.
- Inaccurate information sent to system operators, either to disguise unauthorised changes or to cause operators to initiate inappropriate actions, which could have various negative effects.
- Modified OT software or configuration settings, or OT software infected with malware, which could have various negative effects.
- Interference with the operation of equipment protection systems, which could endanger costly and difficult-to-replace equipment.
- Interference with the operation of safety systems, which could endanger human life.

Considering these then the major security objectives for an OT implementation should include the following [5]:

- **Restrict logical access to the OT network, network activity, and systems.** This may include using unidirectional gateways, utilising a De Militarised Zone (DMZ) network architecture with firewalls to prevent network traffic from passing directly between the corporate and OT networks, and having separate authentication mechanisms and credentials for users of the corporate and OT networks. The OT system should also use a network topology that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.
- **Restrict physical access to the OT network and devices.** Unauthorised physical access to components could cause serious disruption of the OT's functionality. A combination of physical access controls should be used, such as locks, card readers, and/or guards.
- **Protect individual OT components from exploitation.** This includes deploying security patches in as expeditious a manner as possible after testing them under field conditions; disabling all unused ports and services and assuring that they remain disabled; restricting OT user privileges to only those that are required for each user's role; tracking and monitoring audit trails; and using security controls such as antivirus software and file integrity checking software where technically feasible to prevent, deter, detect, and mitigate malware. Keys of OT assets such as PLCs and safety systems should be in the *Run* position at all times unless they are being actively programmed.

- **Restrict unauthorised modification of data.** This includes data that is in transit (at least across network boundaries) and at rest.
- **Detect security events and incidents.** Detecting security events, which have not yet escalated into incidents, can help defenders break the attack chain before attackers attain their objectives. This includes the capability to detect failed OT components, unavailable services, and exhausted resources that are important to provide proper and safe functioning of the OT system.
- **Maintain functionality during adverse conditions.** This involves designing the OT system so that each critical component has a redundant counterpart. Additionally, if a component fails, it should fail in a manner that does not generate unnecessary traffic on the OT or other networks, nor causes another problem elsewhere, such as a cascading event. The OT system should also allow for graceful degradation such as moving from *normal operation* with full automation to *emergency operation* with operators more involved and less automation to "manual operation" with no automation.
- **Restore the system after an incident.** Incidents are inevitable and an incident response plan is essential. A major characteristic of a good security program is how quickly the system can be recovered after an incident has occurred.

To properly address security in an OT system, it is essential for a cross-functional cybersecurity team to share their varied domain knowledge and experience to evaluate and mitigate risk to the OT system. The cybersecurity team should consist of a member of the organisation’s IT staff, control engineer, control system operator, network and system security expert, a member of the management staff, and a member of the physical security department at a minimum. For continuity and completeness, the cybersecurity team should consult with the control system vendor and/or system integrator as well. The cybersecurity team should coordinate closely with site management and the Chief Information Officer (CIO) or Chief Security Officer (CSO), who in turn, along with the Chief Executive Officer (CEO) or Chief Operating Officer (COO), accepts complete responsibility and accountability for the cybersecurity of the OT system and for any safety incidents, reliability incidents, or equipment damage caused directly or indirectly by cyber incidents. An effective cybersecurity programme for an OT system should apply a strategy known as Defence-in-Depth (DiD) layering security mechanisms such that the impact of a failure in any one mechanism is minimised. Organisations should not rely on *security by obscurity*. Which unfortunately was the model employed by OT in the past, the idea of *Air gapped* systems disconnected from the Internet.

A DiD strategy includes [5] :

1. Developing security policies, procedures, training and educational material that apply specifically to the OT system.
2. Considering OT security policies and procedures based on the National Cyber Security Centre (NCSC) advisories, deploying increasingly heightened security postures as the threat level increases.

3. Addressing security throughout the life cycle of the OT system, including architecture design, procurement, installation, maintenance, and decommissioning.
4. Implementing a network topology for the OT system that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.
5. Providing logical separation between the corporate and OT networks (e.g., stateful inspection firewall(s) between the networks, unidirectional gateways).
6. Employing a De-Militarised Zone (DMZ) network architecture (e.g., prevent direct traffic between the corporate and OT networks).
7. Ensuring that critical components are redundant and are on redundant networks.
8. Designing critical systems for graceful degradation (fault tolerant) to prevent catastrophic cascading events.
9. Disabling unused ports and services on OT devices after assuring through testing that it will not impact OT operation.
10. Restricting physical access to the OT network and devices.
11. Restricting OT user privileges to only those that are required to perform each user's function (e.g., establishing role-based access control, configuring each role based on the principle of least privilege).
12. Using separate authentication mechanisms and credentials for users of the OT network and the corporate network (i.e., OT network accounts do not use corporate network user accounts).
13. Using modern technology, such as smart cards for user authentication.
14. Implementing security controls such as intrusion detection software, antivirus software and file integrity checking software, where technically feasible, to prevent, deter, detect, and mitigate the introduction, exposure, and propagation of malicious software to, within, and from the OT system.
15. Applying security techniques such as encryption and/or cryptographic hashes to OT data storage and communications where determined appropriate.
16. Expeditiously deploying security patches after testing all patches under field conditions on a test system if possible, before installation on the OT system.
17. Tracking and monitoring audit trails on critical areas of the OT system.
18. Employing reliable and secure network protocols and services where feasible.

A good reference is the US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organisations to OT [6].

15 Industrial Security: Inverting the CIA Triad

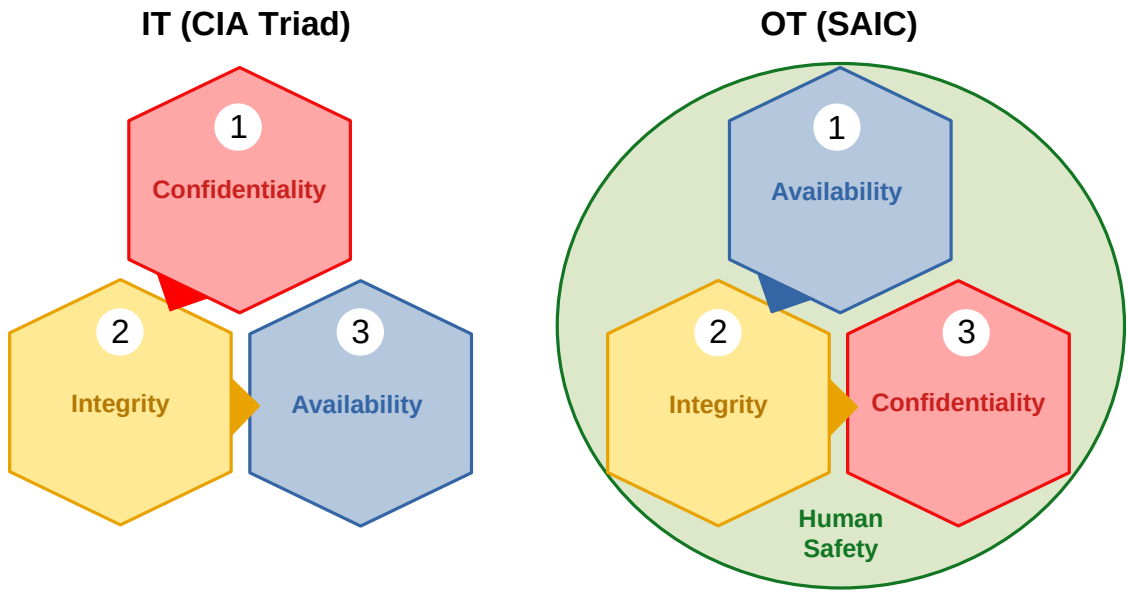

Figure 16: Inverting the CIA Triad

For many years, information security has held Confidentiality, Integrity and Availability (known as the CIA triad) as the core principles of information security.

15.1 Confidentiality

Confidentiality is the term used to prevent the disclosure of information to unauthorised individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorised party obtains the card number in any way, a breach of confidentiality has occurred.

Breaches of confidentiality take many forms. Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality. If a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in a breach of confidentiality. Giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorised to have the information.

Confidentiality is necessary (but not sufficient) for maintaining the privacy of the people whose personal information a system holds.

15.2 Integrity

In information security, integrity means that data cannot be modified without authorisation. This is not the same thing as referential integrity in databases. Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorised user vandalises a web site, when someone is able to cast a very large number of votes in an online poll, and so on.

There are many ways in which integrity could be violated without malicious intent. In the simplest case, a user on a system could miss-type someone's address. On a larger scale, if an automated process is not written and tested correctly, bulk updates to a database could alter data in an incorrect way, leaving the integrity of the data compromised. Information security professionals are tasked with finding ways to implement controls that prevent errors of integrity.

15.3 Availability

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.

15.4 Safety, Availability, Integrity, Confidentiality for OT

Security was not initially considered as an important factor when designing an ICS. In fact, often, it was not considered because of the fear that implementing security controls could reduce the availability of the system. For example, in a case where a power station is continually producing power, then any stoppage has a big impact to the process. Stopping and starting a complete power station process can take significant time, so undertaking a patch that involves restarting a critical device may have to wait for days, weeks or event months before a patch window might be given.

Therefore the IT core principals of the Confidentiality, Integrity and Availability (CIA), the CIA triangle, with confidentiality being the most important, is completely inverted when OT systems are considered. First and foremost is Human Safety, then the Availability of the system, closely followed by Integrity, are far more important than Confidentiality in this case, the Safety, Availability, Integrity, Confidentiality (SAIC).

15.4.1 Example

Figure 17: Brewery

A breweries main Production Management Software (PMS), actually running outside of the IACS, in the enterprise network, was affected by malware. Because the production management system was down, the production line had to be halted. Because the production line was stopped, no product is coming off the line that could be packed and shipped. The resulting logjam, then also means that goods coming in can not be unloaded, and production line employees are unable to do their jobs.

This is why Availability is more important than Confidentiality in OT.

Data however is still very important within OT as proprietary knowledge and confidential product information can all be stored and transmitted as part of a OT network.

In the brewery, the recipes and process timings have to be stored, and security controls, by necessity, have to be focused on keeping production running, but also on protecting companies intellectual property that are also likely to be on the network.

16 Bibliography

[1] Directive (EU) 2022/2555, *Measures to ensure a high common level of cybersecurity in the Union and amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing the Directive (EU) 2016/1148 (NIS 2 Directive)*. 2022, p. 73. Accessed: Aug. 08, 2022. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[2] Directive (EU) 2022/2557, *EU The resilience of critical entities and repealing Council Directive 2008/114/EC*. 2022, p. 73. Accessed: Aug. 08, 2022. [Online]. Available: http://data.europa.eu/eli/dir/2022/2557/oj

[3] 'Public Summary of Sector Security and Resilience Plans'. UK Cabinet Office, Feb. 01, 2019. Accessed: Aug. 08, 2023. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786206/20190215_PublicSummaryOfSectorSecurityAndResiliencePlans2018.pdf

[4] L. F. Menabrea and A. Lovelace, 'Sketch of The Analytical Engine', *Bibliothèque Universelle de Genève*, Oct. 1842, Accessed: Aug. 08, 2023. [Online]. Available: https://www.fourmilab.ch/babbage/sketch.html

[5] 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

[6] 'Security and Privacy Controls for Information Systems and Organizations to OT', National Institute of Standards and Technology, NIST SP 800-53 Rev. 5, 2020. Accessed: Aug. 08, 2023. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-53r5

This page is intentionally blank