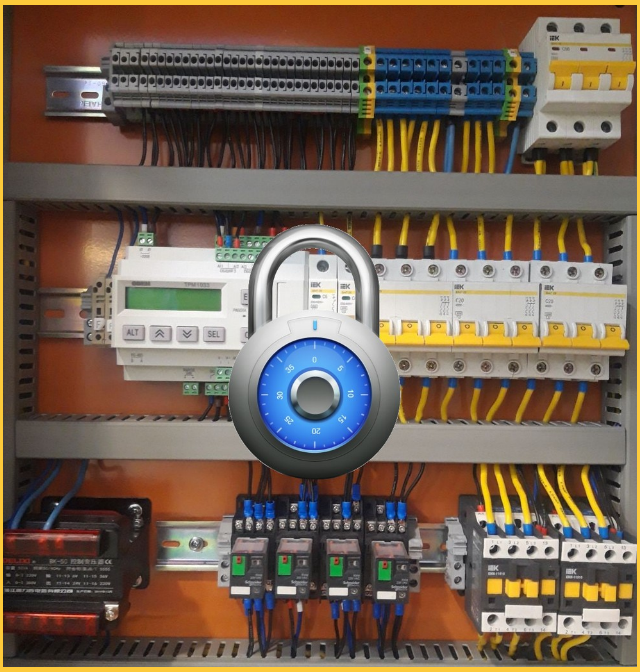
Exercise 1

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

This page is intentionally blank

1 Exploring OT

1.1 Exercise #1 - IACS at an Electrical Power Plant

Scenario Consider a gas powered electricity generation plant near a major urban city. The power industry is susceptible to security vulnerabilities as it adopts digital communication methods that help make energy production and distribution more efficient. Much of how we live and work globally is dependent upon electricity, including everyday cooking, heating, cooling, but also in this case, of the electrical power consumed is also derived from gas. Even the smallest cyber attack on one of the thousands of inter-connected systems used to generate and distribute the electricity can pose a serious cyber risk. Any electrical company that goes through an attack could experience a plant shutdown, equipment damage, utility interruptions, production shutdown, inappropriate product quality, undetected gas leaks and safety measure violations, to name but a few. The numerous cyber attacks on the Ukrainian electricity grid over the last decade demonstrate the vulnerability of local populations to such attacks. This was ramped up and the fear generated by attacks near the Zaporizhzhia nuclear plant as a result of the war between Russia and Ukraine. Europe has been extremely lucky that the electricity generation has largely avoided devastating data breaches. However, this does not diminish the risk factor. In fact, when you consider the context of power stations such as this one, nestled near an urban environment, the overall risk to human life can increase substantially. In the EU Electricity is considered critical infrastructure. This is defined as electricity undertakings which carry out the function of ‘supply’. This includes;

- Distribution system operators
- Transmission system operators
- Producers
- Electricity market operators
- Market participants providing aggregation, demand response or energy storage services
- Operators of a recharging point that are responsible for the management and operation of a recharging point, which provides a recharging service to end users, including in the name and on behalf of a mobility service provider.

Power generation and distribution is a complex operation which may have legacy equipment, massive facilities with hundreds of locations and thousands of PLC devices in panels with some at a potential high-risk location. Where do you start? Let us first start by looking at the top OT cyber vulnerabilities affecting OT.

- Attrition of Network Architecture
- Lack of homogeneous ownership
- Poor visibility
- IoT Bots and DDoS attacks
- Use of removable media
- The security posture of sub-components
- Human Error

- Connecting to the cloud
- OT and IT Convergence
- Lack of awareness

Break this down a bit more and think through the implications from two primary perspectives, IT and OT.

1.2 The OT Perspective

Start with some key observations from the OT perspective. When you explore and evaluate facilities, like power generation plants from an OT perspective, it is likely that a mixture of systems that have often evolved organically will be found, as the technology options have expanded. For example; legacy SCADA systems, fully automated processing systems, or typical OT environmental systems like Heating, Ventilation, and Air Conditioning (HVAC), power, water, battery backup, etc. can be found. In some cases, these systems might be automated, but many are still manual systems. Pressure and temperature sensors, not to mention distribution systems and their associated sensors and controls will be found. There are also safety control systems, physical security systems, cameras, badge access, gate access, etc. All these systems are typically monitored in some fashion, which means network connectivity by any means necessary. There is a lot to explore in these environments and much to assess and evaluate. The size of these facilities adds more challenges because typical OT environments will have PLC panels located inside and out, which could be spread far and wide. Most of these panels are housed on serial networks with some sort of converter or switch to go from serial to Ethernet and are then often connected to a WiFi router. Each panel, its location, and its connections, all present their own set of risks. Being able to assess those risks will help mitigate disaster.

Continuing through this scenario, consider using both the OT and IT perspectives to help with that risk assessment and management. Here are some examples of what could be found during IACS assessment of an power generation plant.

Legacy control processing station

This monitors show the flow of power as well as power level readings. This is a good example of a SCADA monitoring industrial control station.

Modern control system

A modern control system contains applications that typically run on top of an operating system such as Microsoft Windows or Linux. As such, this control system is connected via a local area network. With this type of connectivity, and the fact that most operating systems of this type can't be patched, updated or improved, the area of risk is greater. The greater the automation, the greater the risk.

PLC panel

A control PLC can include an embedded web server gray box, also called a thin server. A serial cable connecting the web server to the PLC for data exchange is often employed, as well as an Ethernet Local Area Network (LAN) connection for WiFi to the Internet.

Visual screen

PLC panels are likely to have a visual screen on the panel door that shows the condition of process.

1.3 Question #1: Facility Footprint

Why is the size of an electricity generation plant relevant?

a) The larger the footprint, the more networking connectivity required, hence more Assets to monitor and protect
b) The larger the footprint, the greater use of Wi-Fi networking
c) The larger the footprint, the more physical security controls needed
d) All of the above

1.3.1 Answer

(d) All of the above. The size of an electricity generation plant is relevant to cybersecurity for all of the following reasons:

- **More networking connectivity**: Larger plants have a larger footprint, which means they require more networking connectivity to connect all of the different systems and devices. This increased connectivity also creates more potential attack surfaces for cyber attackers to exploit.
- **Greater use of Wi-Fi networking**: Wi-Fi networking is often used in larger plants to provide wireless connectivity for employees and devices. However, Wi-Fi networks are more vulnerable to cyber attacks than wired networks.
- **More physical security controls needed**: Larger plants have more physical assets to protect, which means they need more physical security controls in place. However, physical security controls can also create vulnerabilities in cybersecurity, such as if they are not properly configured or maintained.
- In addition to these factors, larger plants may also have more complex operational systems and processes, which can make them more difficult to secure.

Here are some specific examples

- A larger plant may have more Remote Terminal Units (RTU) and other Industrial Automation & Control Systems (IACS) devices. These devices are often critical to the operation of the plant, and they can be vulnerable to cyber attacks.
- A larger plant may have more complex substation automation systems. These systems are responsible for controlling the flow of electricity to and from the plant, and they can be targeted by cyber attackers to cause widespread power outages.
- A larger plant may have more employees and contractors with access to its systems. This increased access to systems creates more opportunities for human error and social engineering attacks.
- Overall, the size of an electricity generation plant is a significant factor to consider when developing and implementing a cybersecurity programme. Larger plants face a number of unique challenges, and they need to take steps to mitigate these risks.

2 Digitisation of IACS Environments

Continuing with the OT Perspective consider taking a closer look at how legacy systems can regularly persist in IACS/OT environments, especially in many electrical generation facilities. In some cases, the equipment dates to the 1960s. This ageing equipment is typically monitored by an ageing Windows workstation, often running something such as Win XP. Without a broader cybersecurity industry standard, examples like this are still normal. It is even possible to find other control modules that are still running Windows 95 and Windows 98. Remember, these systems are plugged into control modules on SCADA systems that cannot be updated. To their credit, these SCADA systems continue to work very well even though they present a risk.

To address the challenge of outdated equipment, there is often cases where technology leapfrogs, or jumps over phases of technological advancement. An example such as an embedded web server on a PLC panel. The relatively modern embedded web server allows for easy, streamlined remote monitoring and management of a power system. That allows a single technician in the control room to monitor the power systems across the facility. One person can now access the machine equipment at the thin server's assigned IP address. An application such as a Statistical Process Control (SPC) package, can now take advantage of two-way data exchange with the equipment. The access to information is useful and more efficient in the administration of the plant, but it also presents some additional risk to the IACS equipment and OT operations. How? Web servers that are connected to networks can be accessed remotely, and could therefore be attacked, infiltrated, or disabled. There is no doubt that the energy sector will benefit from digitisation, but the scramble to retrofit decades-old power facilities will take time and millions of Euros to execute. And as that transformation takes place, the cybersecurity vulnerabilities and risks must be considered.

2.1 Question #2: Securing Legacy Systems

Consider an electricity power generation plant with legacy control systems with Windows XP monitoring/control stations. They cannot be upgraded or touched in any way. What is the most optimal method for securing these assets?

a) Place these assets on an isolated VLAN network
b) Create a zone that is specific to the operational requirement and then restrict connectivity between zones
c) Add Anti-virus software to workstations
d) Upgrade to the latest version of Windows OS

2.1.1 Answer

(a) Place these assets on an isolated VLAN network: The most optimal method for securing legacy control systems with Windows XP monitoring/control stations that cannot be upgraded or touched in any way is to place them on an isolated VLAN network.

A VLAN network is a virtual local area network that allows you to segment your network into multiple isolated networks. This can be a very effective way to improve security by restricting traffic flow between different parts of your network.

In the case of an electricity power generation plant with legacy control systems with Windows XP monitoring/control stations, placing these assets on an isolated VLAN network would help to protect them from cyber attacks by making them more difficult to access for attackers. Here are some of the benefits of placing legacy control systems on an isolated VLAN network:

- It reduces the attack surface by restricting traffic flow to and from the VLAN.
- It makes it more difficult for attackers to move laterally within the network.
- It simplifies security management by allowing you to apply security controls to specific VLANs.

Here are some additional steps that can be taken to improve the security of legacy control systems:

- Implement strong password policies and require regular password changes.
- Use multi-factor authentication for all remote access to legacy control systems.
- Install and maintain up-to-date security software on all workstations and servers.
- Implement a security monitoring programme to detect and respond to cyber attacks.

It is important to note that even though legacy control systems cannot be upgraded, there are still steps that can be taken to improve their security. By following the steps above, electricity power generation plants can help to protect their critical infrastructure from cyber attacks.

3 Distributed Control Systems

As mentioned, electricity power generation plants are large-scale plants that produce large electrical outputs and feature a complicated production process with a great number of devices and equipment. Because of the high capacity, these facilities operate continuously for long periods of time. Of course, this means hundreds of sensors, values, and equipment. All of this has to be monitored somewhere. In the IT environments, this would generally be associated with an Network Operations Centre (NOC). In OT environments, this typically refers to a control room with a Distributed Control System (DCS). A DCS, first emerged in large high value, safety critical process industries, and were attractive because the DCS manufacturer would supply both the local control level and central supervisory equipment as an integrated package, thus reducing design integration risk. Today, the functionality of SCADA and DCS systems are very similar, but DCS tends to be used on large continuous process plants, like an electricity power generation plants and distribution systems, where high reliability and security is important, and the control room is not geographically remote. The key attribute of a DCS is its reliability due to the distribution of the control processing around nodes in the system. These are the PLC panels we discussed earlier.

Figure 1 is a general model which shows functional manufacturing levels using computerised control. Referring to the diagram,

- **Level 0** contains the field devices such as flow and temperature sensors and final control elements such as control valves.
- **Level 1** contains the industrialised Input/Output, I/O, modules and their associated distributed electronic processors.
- **Level 2** contains the supervisory computers which collect information from processor nodes on the system and provide the operator control screens.
- **Level 3** is the production control level, which does not directly control the process but is concerned with monitoring production and monitoring targets.
- **Level 4** is the production scheduling level.

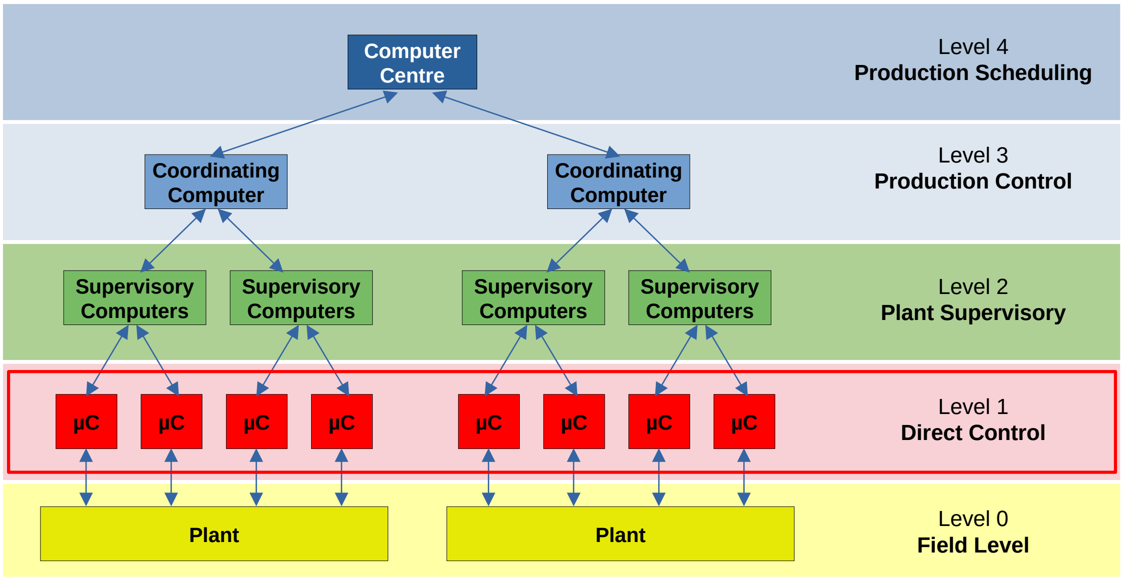


Figure 1: Functional manufacturing levels using computerised control

Process control of large industrial plants, like an electrical power generation plant, has evolved through many stages. Initially, control would be from panels local throughout the facility, however, this required a large manpower resource to attend these dispersed panels, and there was no overall view of the process. The next logical development was the transmission of all plant measurements to a permanently manned central control room. With the coming of electronic processors and graphic displays, it became possible to replace these discreet controllers with computer-based algorithms hosted on a network of Input/Output racks with their own control processors. These could be distributed around the facility and communicate with the graphic display in the control rooms. The distributed control system was born. The introduction of DCS allowed easy interconnection and reconfiguration of plant controls such as cascaded loops and interlocks, and easy interfacing with other production computer systems. It enabled sophisticated alarm handling, introduced automatic event logging, removed the need for physical records such as chart recorders, allowed the control racks to be networked and thereby located locally to the plant to reduce cabling runs, and provided high-level overviews of operation status and production levels. While OT operations, safety controls, and physical controls are monitored, cybersecurity is rarely discussed. However, if the deployment of cybersecurity measures can't keep pace in an environment with high levels of criticality, then what compensating measures can be put in place? This is where risk management comes into play.

3.1 Question #3: OT Vulnerabilities

Which of these is a TOP vulnerability impacting OT cybersecurity?

a) The use of Unmanaged Desktops and Laptops
b) The use of vulnerable Software
c) Monitoring of OT Systems
d) Cybersecurity training

3.1.1 Answer

(b) The use of vulnerable Software: The most optimal method for securing legacy control systems with Windows XP monitoring/control stations that cannot be upgraded or touched in any way is to place them on an isolated VLAN network. This is because OT systems often use legacy software that is no longer supported by the vendor. This software is often vulnerable to known and unknown security vulnerabilities, which can be exploited by attackers to gain access to and disrupt OT systems. The other options are not as critical for OT cybersecurity as the use of vulnerable software:

(a) **The use of Unmanaged Desktops and Laptops**: Unmanaged desktops and laptops can pose a security risk to OT systems if they are used to access OT networks or systems. However, this risk can be mitigated by implementing strong network segmentation and access control measures.

(c) **Monitoring of OT Systems**: Monitoring of OT systems is important for detecting and responding to cyber attacks. However, it is not a vulnerability in itself.

(d) **Cybersecurity training**: Cybersecurity training is important for all employees, including those who work with OT systems. However, it is not a vulnerability in itself.

It is important to note that all of the options listed above can contribute to OT cybersecurity risks. However, the use of vulnerable software is the TOP vulnerability impacting OT cybersecurity because it is the most common and exploitable vulnerability.

Here are some tips for mitigating the risk of using vulnerable software in OT systems:

- Identify all OT systems and the software they are using.
- Assess the vulnerability risk of all OT software.
- Prioritise patching and updating OT software to the latest version.
- Implement strong network segmentation and access control measures to protect OT systems from vulnerable software.
- Deploy security solutions such as firewalls and intrusion detection systems to protect OT systems from known and unknown security vulnerabilities.

4 Risk Management

Now, consider this from an IT perspective. This can feel like a shift in thinking, but the key concept here is that OT and IT need to work together. An OT professional has to think from both perspectives constantly. By remaining in one mindset or the other, it is not possible to address the situations that often occur in OT environments. Remember the reviewed OT environments with very outdated operating systems? That would rarely happen in an IT perspective because in IT there is constant installing, maintaining, and securing desktops, laptops, etc.. IT are also administering and securing office productivity applications such as Office suites. IT are immersed in Cloud environments such as Amazon Web Services (AWS), Google Cloud Platform (GCP), or Microsoft Azure. These systems are complex, but they are usually not connected to physical interfaces that control the flow of liquids, for example. The risks presented in typical IT environments are very different, but common process can be used to address risk in all environments. Enterprise Risk Management (ERM), is the process of planning, organising, leading, and controlling the activities of an organisation in order to minimise the effects of risk on an organisation's capital and earnings. An IT security or IT operations person needs to adapt and apply not only the OT security infrastructure and architecture, but also the core aspects of risk management into the overall IACS cyber security programme. It's about protecting revenue while maintaining operational availability. This is not an easy balancing act, but it is critical to understand and practice as you develop your IACS skillset.

4.1 Question #4: Managing Risk in IT and OT

As an IT Security or IT Operations person coming into and IACS Cybersecurity environment, what is your primary goal?

a) Protect Assets and Reduce Risk
b) Protect Revenue while maintaining Operational Availability
c) Measure the risks and Control them, then see where you can improve your process
d) Find the potential risks, measure those risks, set acceptable limits for the risk, review and re-examine those limits, then repeat
e) Find the potential risks, then control them, then assess them, after that you can relax a bit
f) Control risk at all times and in all situations, then measure it, then review that measurement and then find possible risks

4.1.1 Answer

(a) Protect Assets and Reduce Risk : IACS systems are critical to the operation of critical infrastructure, and they are increasingly being targeted by cyber attackers. By protecting assets and reducing risk, you can help to ensure the continued operation of critical infrastructure and protect the public from harm. Here are some specific steps you can take to protect assets and reduce risk in an IACS Cybersecurity environment:

- Identify and classify all IACS assets.
- Assess the vulnerability and threat risks to IACS assets.
- Implement appropriate security controls to mitigate risks.
- Monitor IACS systems for suspicious activity and respond to incidents promptly.
- Develop and implement an IACS Cybersecurity incident response plan.

In addition to these steps, it is also important to work with other stakeholders, such as business leaders and operational personnel, to ensure that IACS Cybersecurity is integrated into the overall enterprise risk management programme. The other options are not as accurate or comprehensive as the primary goal of protecting assets and reducing risk in an IACS Cybersecurity environment:

(b) Protect Revenue while maintaining Operational Availability: This is an important goal, but it is not the primary goal of IACS Cybersecurity. The primary goal is to protect assets and reduce risk, even if this means taking some downtime to implement security controls or respond to incidents.

(c) Measure the risks and Control them, then see where you can improve your process: This is a good step in the IACS Cybersecurity process, but it is not the primary goal.

(d) Find the potential risks, measure those risks, set acceptable limits for the risk, review and re-examine those limits, then repeat: This is a good description of the Enterprise Risk Management cycle, but it is not the primary goal of IACS Cybersecurity.

(e) Find the potential risks, then control them, then assess them, after that you can relax a bit: This is not an accurate or comprehensive description of the IACS Cybersecurity process.

(f) Control risk at all times and in all situations, then measure it, then review that measurement and then find possible risks: This is not a realistic or achievable goal for IACS Cybersecurity.

It is important to note that IACS Cybersecurity is a complex and challenging field. There is no one-size-fits-all solution, and the best approach will vary depending on the specific organization and IACS environment. However, by focusing on the primary goal of protecting assets and reducing risk, you can help to ensure the security of IACS systems and the critical infrastructure they support.

5 Perspectives from the Field: Inverting the CIA Triangle

There can be a disconnect between the OT side of an operation and the IT side. OT is is very segmented, very siloed. As a result both sides tend to remain autonomous from each other. OT does not necessarily consider IT as an extension of their particular operations despite the evidence of major convergence now. IACS type environments are rapidly becoming more Internet Protocol (IP) based. IACS residing on an IT network is a dynamic shift occurring today and it is essential that OT and IT work together. The IT side consider security through the CIA triad while the OT side see Availability as the priority and also include Safety as a priority and even in some cases, such as critical infrastructure, safety comes first. Both IT and OT must work out their joint priorities as the future is automation, and automation will be all IP based. Another consideration is people, people that may have worked in manufacturing and process control for 40 years, now Internet of Things (IOT) and industrial IOT changes the way things work, convergence is happening organically. It is important that people are retrained and continue to have role relevance so as not to become obsolete and disgruntled.

This page is intentionally blank