SETU
Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Bridging the IT/OT Gap: Convergence and the Evolution of Industrial Cyber Defence

Dr Diarmuid Ó Briain

1 Feb 2026

Licence

- Part 1: Operational Technology (OT) Overview
- Part 2: Engineering a Defence
- Part 3: The Adversary's Playbook
- Part 4: Regulation – Network Information Systems (NIS2), Critical Information Infrastructure (CII) and Beyond
- Part 5: Wrap-up

- **Part 1: OT Overview**

Information Technology —v— Operational Technology

- **IT**

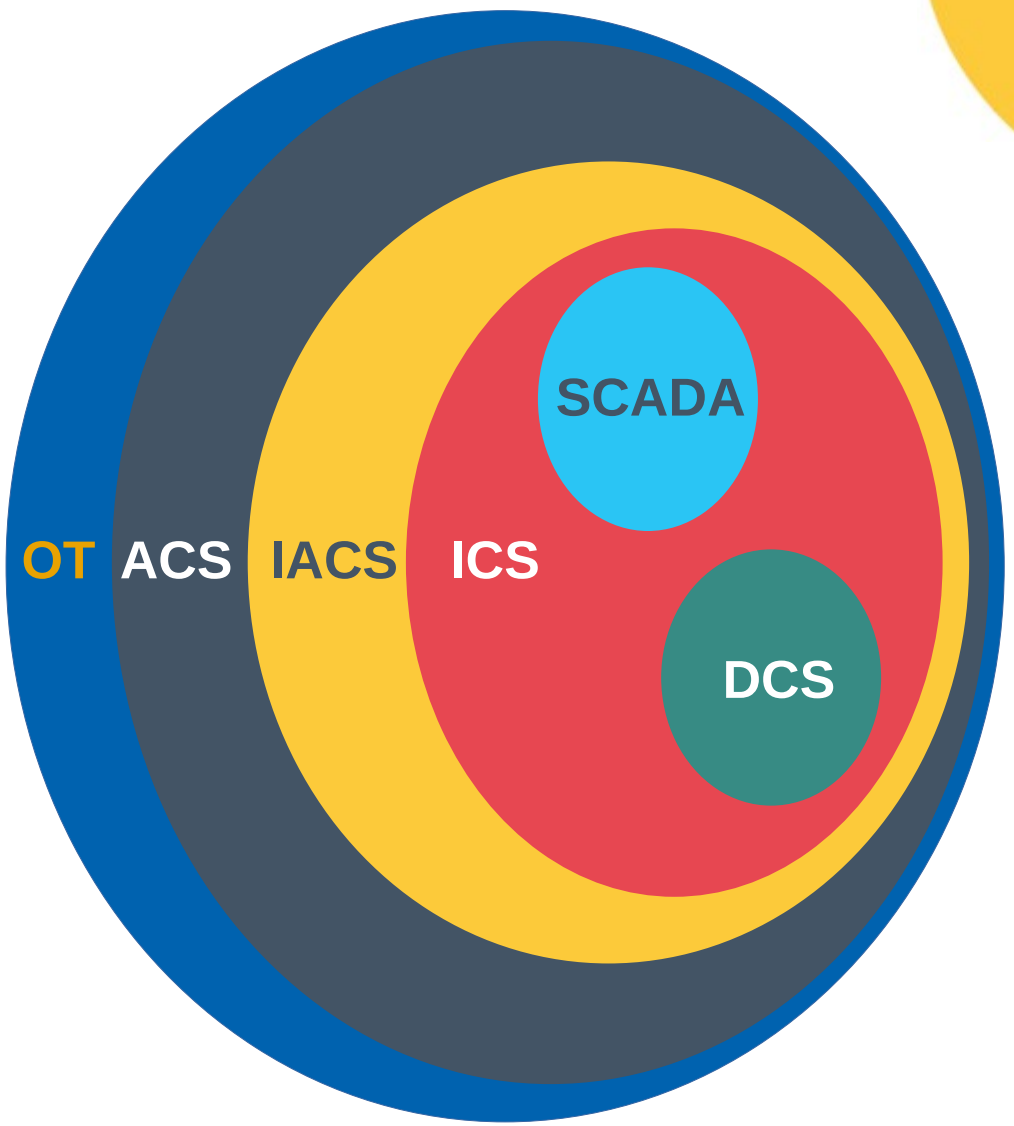
Any equipment or interconnected system used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an organisation or by a 3rd party on the organisations behalf.

- **OT**

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.

Some OT Terms

- Operational Technology (OT)
- Automation and Control Systems (ACS)
- Industrial Automation and Control Systems (IACS)
- Industrial Control Systems (ICS)
- Supervisory Control and Data Acquisition (SCADA)
- Distributed Control System (DCS)



Exercise #1

Exercise #1

- What is different about this power station and a typical office environment in terms of computing?

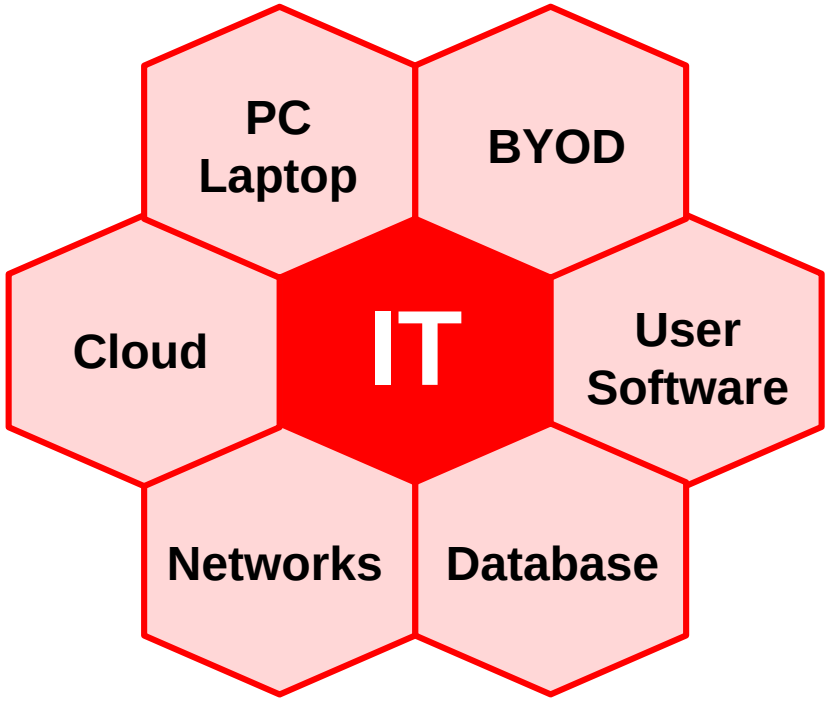
2

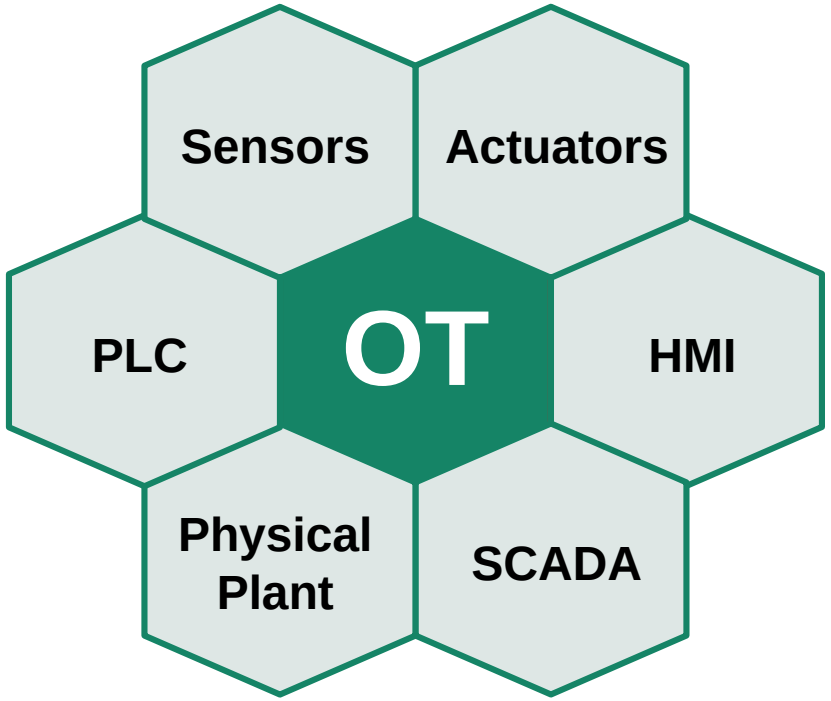
Baglihar Hydroelectric Power

Exercise #1

- What is different about this power station and a typical office environment in terms of computing?
  - Computing interacts with physical processes.
  - There is the potential for physical damage.
  - The size of such facilities and the concerns for operations and security.
  - There is a real risk to human life.
  - Wider implications for society if the station is disrupted.

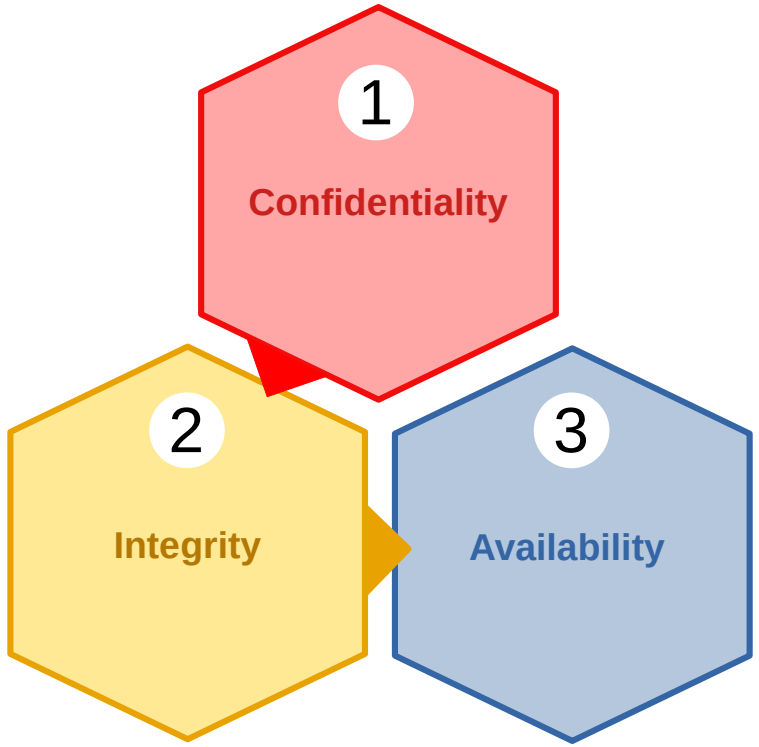
Information Technology -v- Operational Technology





Core Priorities IT/OT

IT (CIA Triad)



OT (SAIC)

Exercise #2

Bev9 Breweries

Exercise #2

- **Bev9 Breweries main Production Management Software (PMS), actually running outside of the IACS, in the enterprise network, was affected by malware.**

What are the implications?

2

Exercise #2

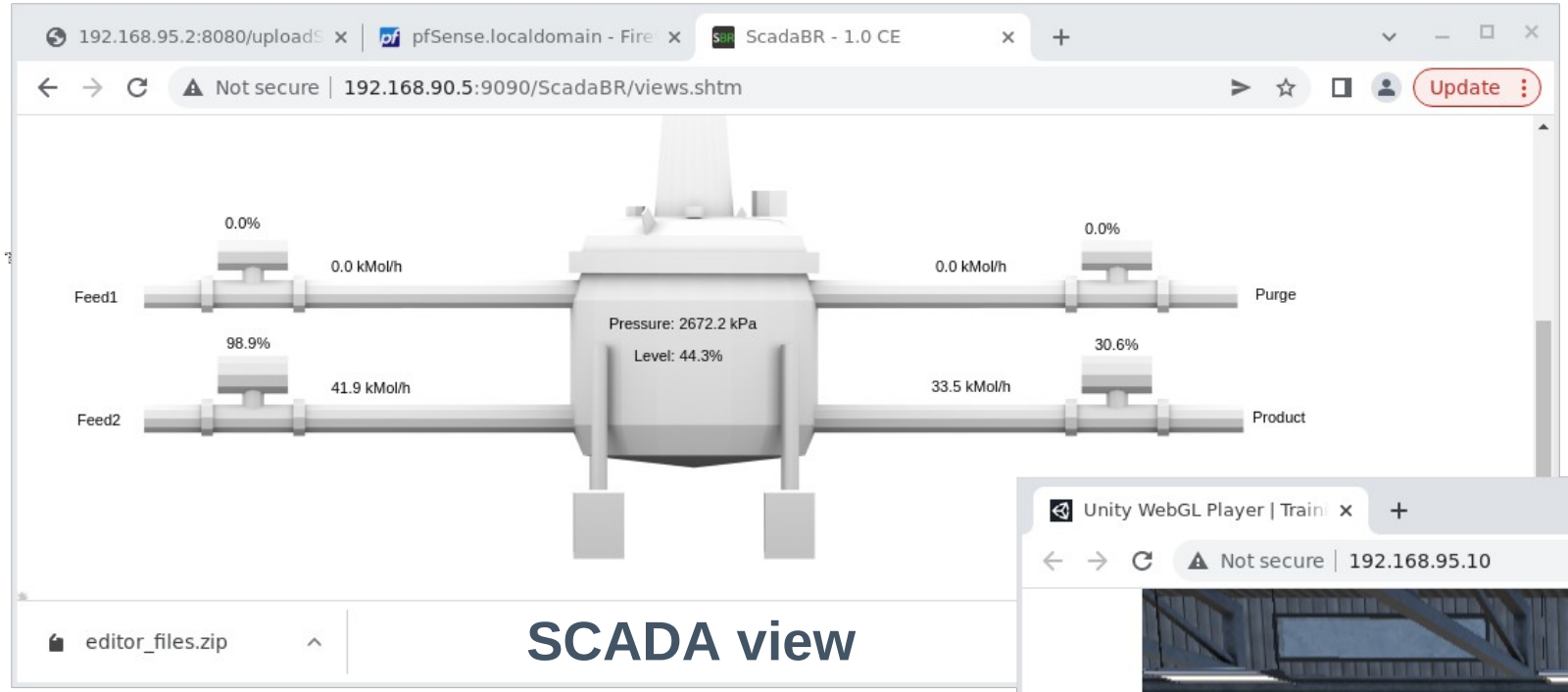
- **Bev9 Breweries main Production Management Software (PMS), actually running outside of the IACS, in the enterprise network, was affected by malware.**
  - Because the PMS was down, the production line had to be halted.
  - Because the production line was stopped, no product was coming off the line that could be packed and shipped.
  - The resulting logjam, then also means that goods coming in cannot be unloaded, and production line employees are unable to do their jobs.

Exercise #2

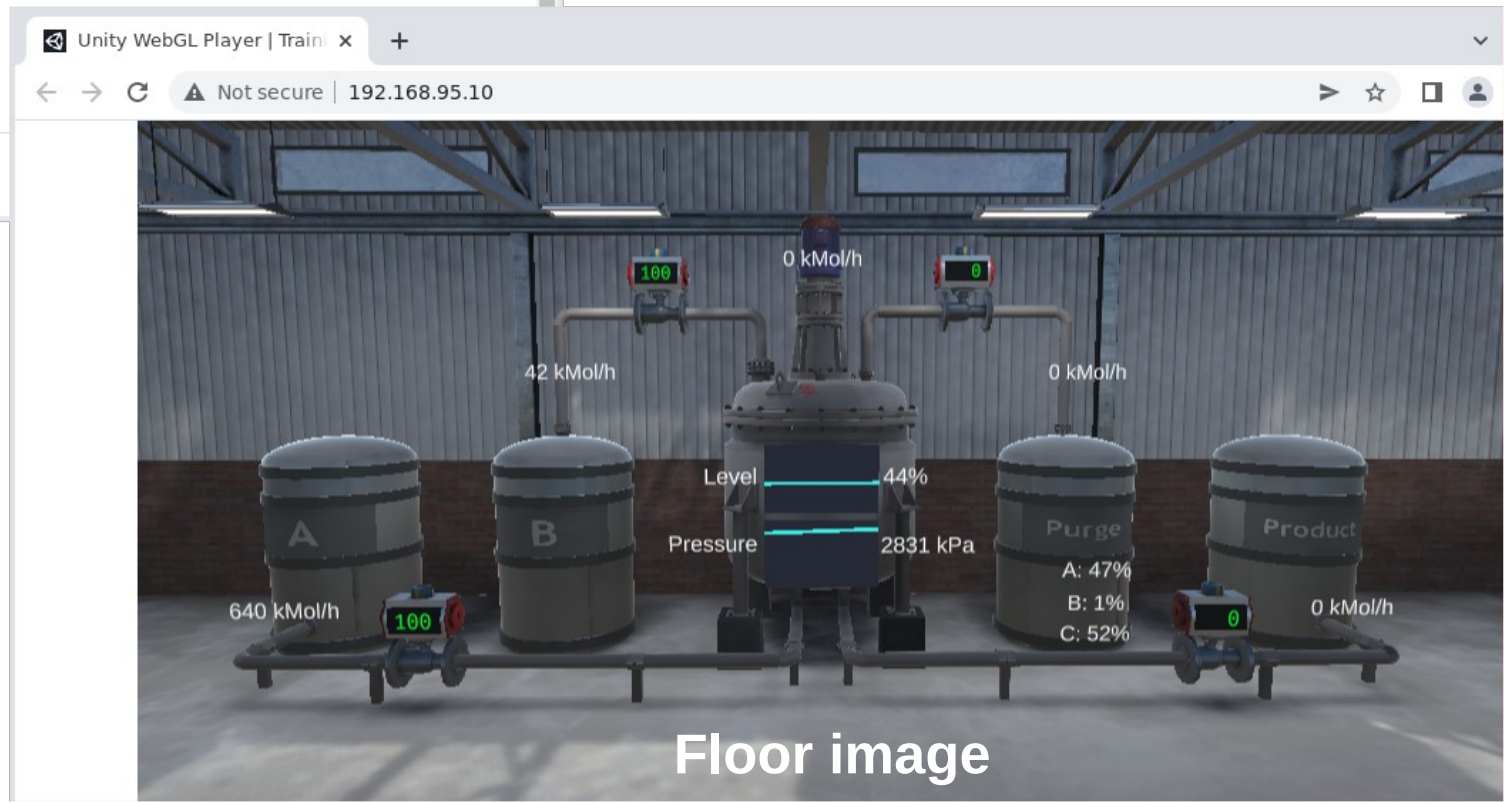
- This is why **Availability** is more important than **Confidentiality** in OT.

- Data 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.
  - Storage of Bev 9 breweries' recipes, process timings, security controls as well as Intellectual Property (IP).

Observe anything?

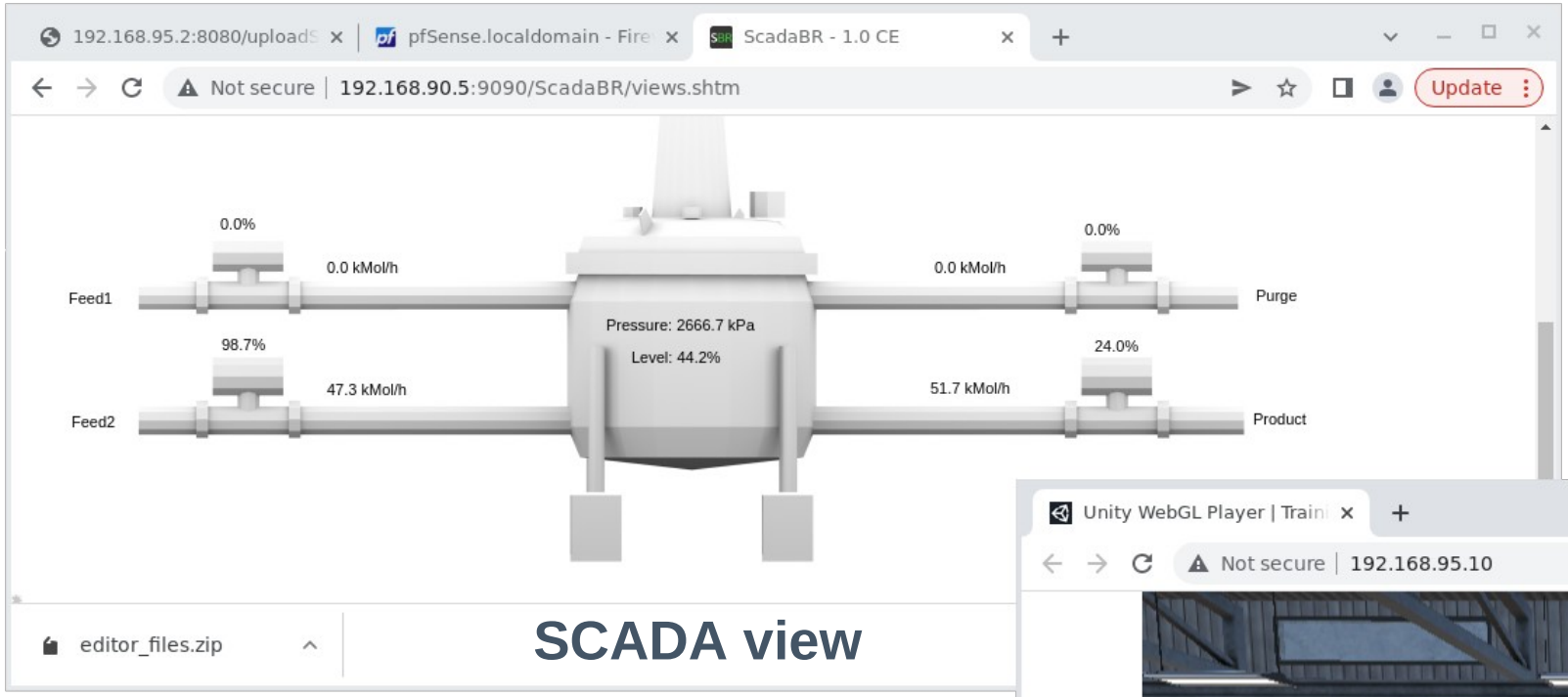


SCADA view

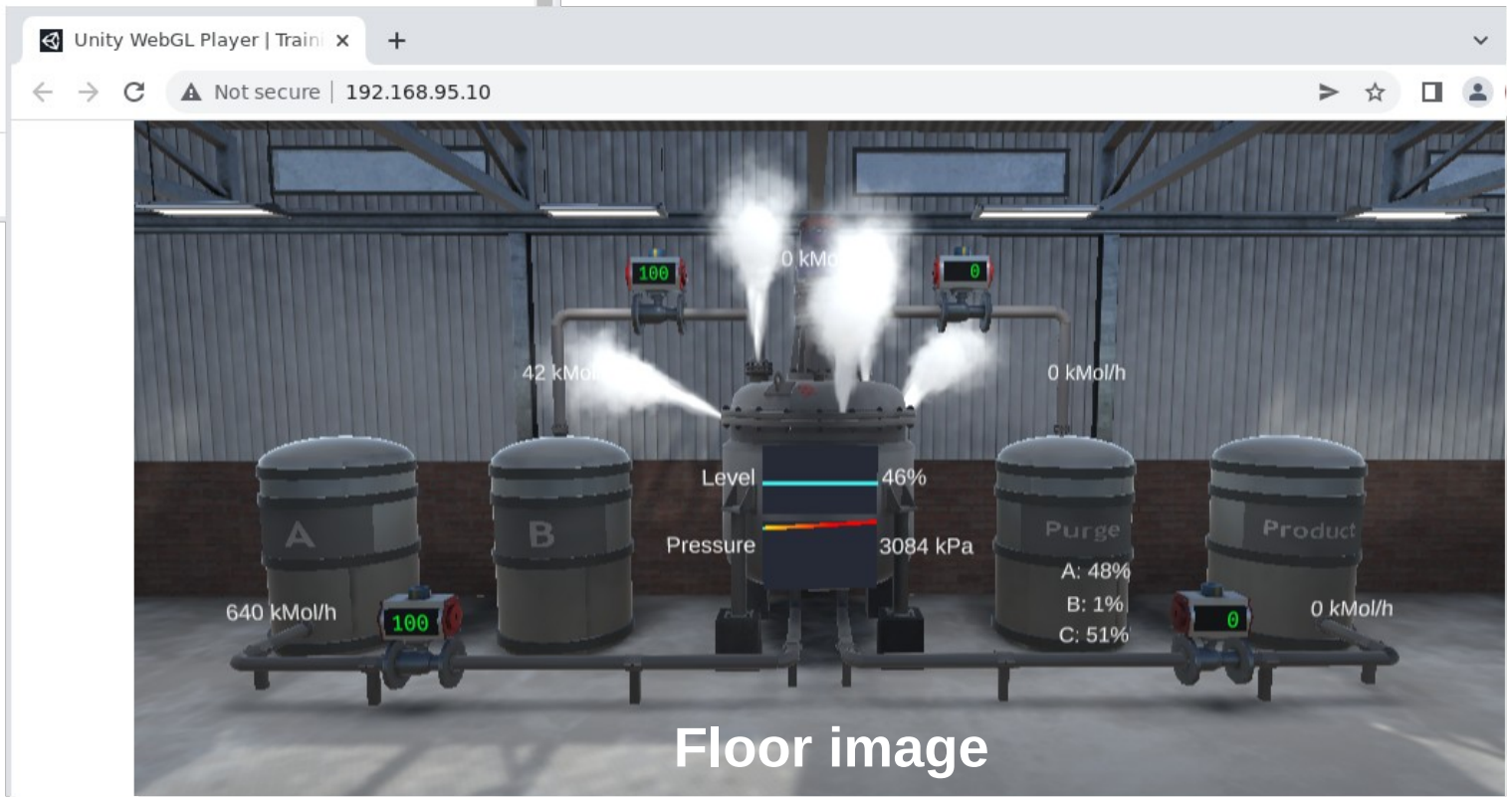


Floor image

1



SCADA view

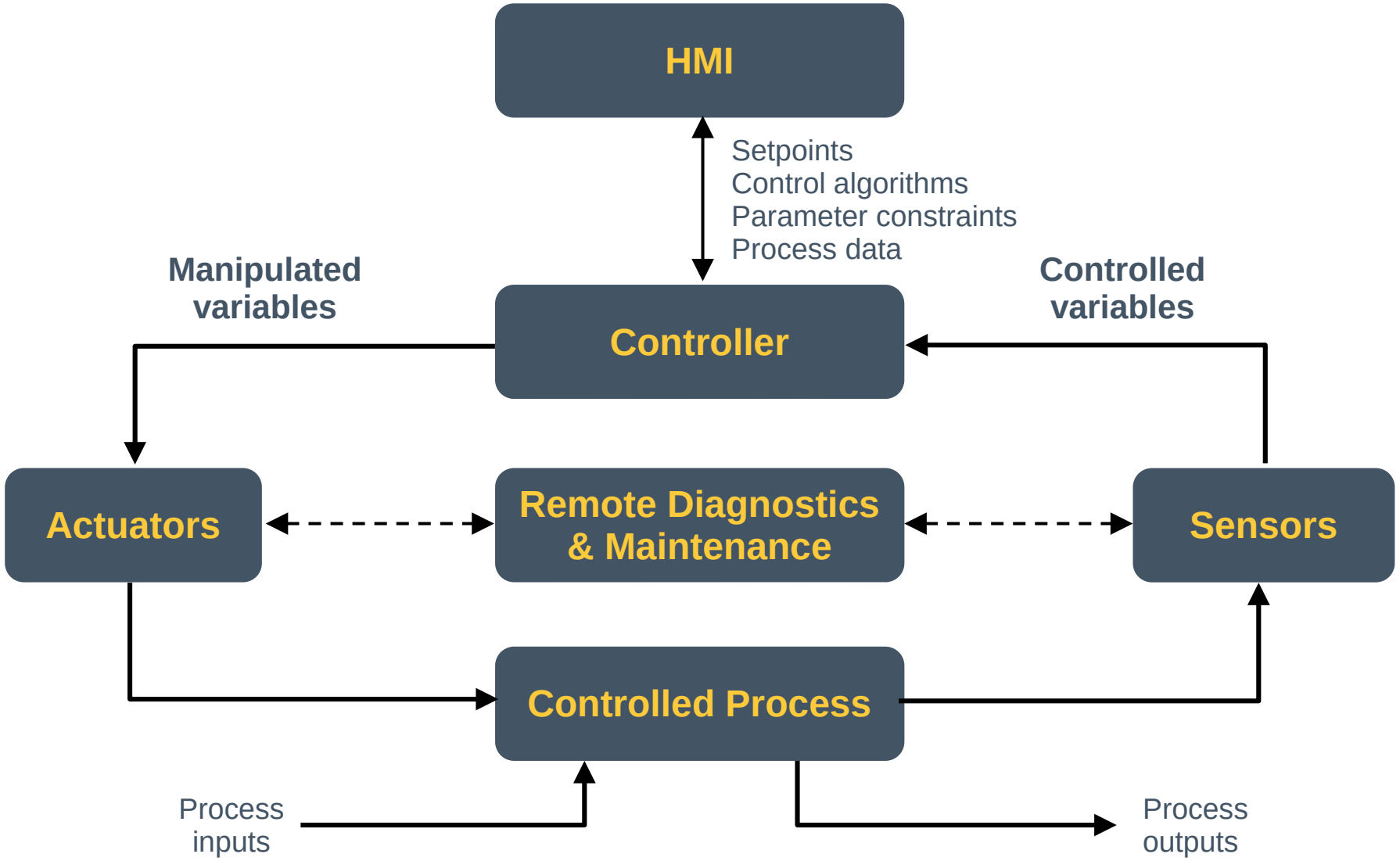


Floor image

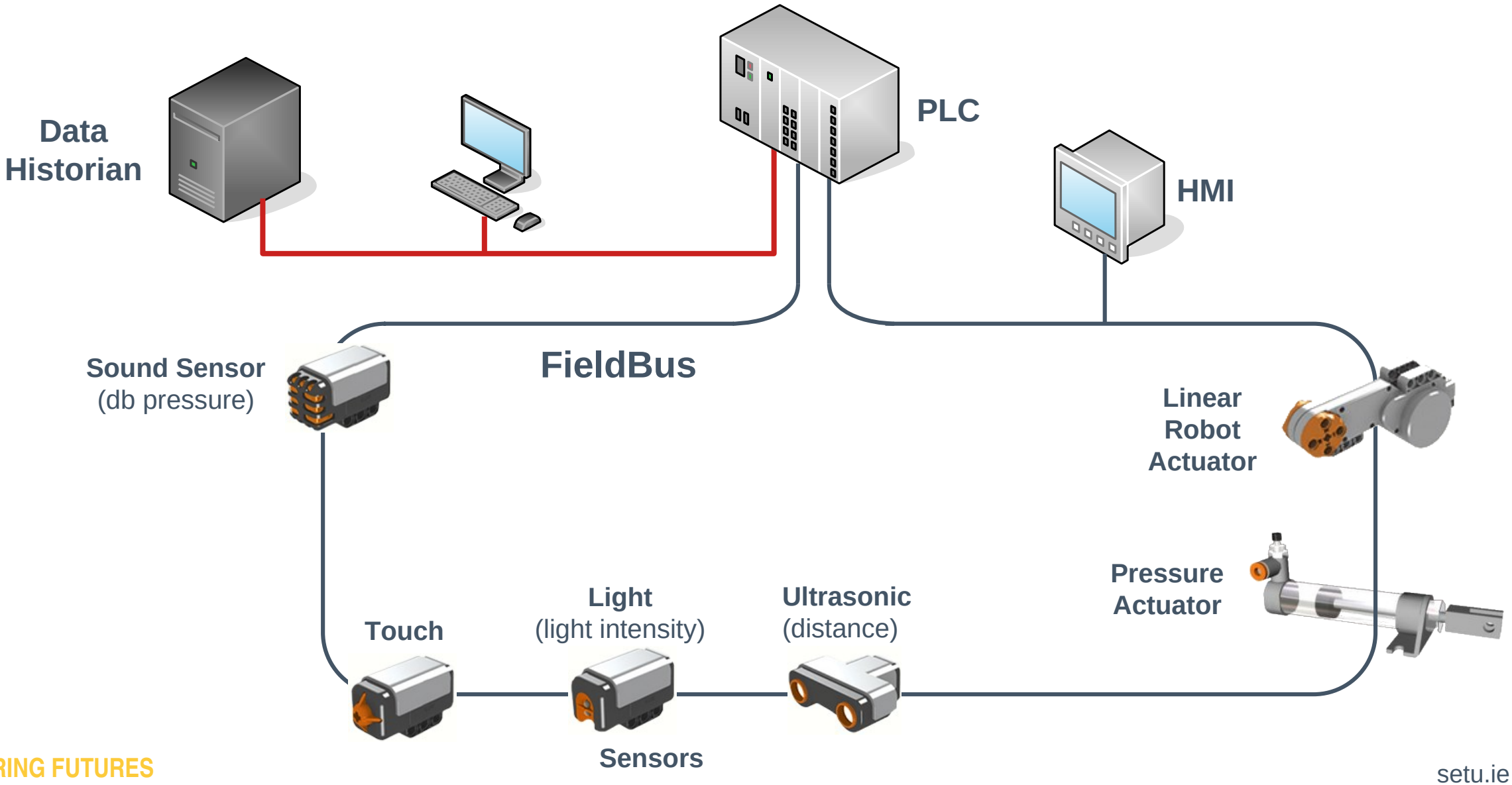
Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Purdue Enterprise Reference Architecture (PERA)

Typical OT System



PLC Control in OT System



Functional manufacturing levels

Enterprise Zone

Enterprise Network — Level 5

Site Business Planning & Logistics Network — Level 4

De-militarised Zone — Level 3.5

Manufacturing Zone

Site Manufacturing Operations & Control — Level 3

Cell/Area Zone

Area Supervisory Control — Level 2

Basic Control — Level 1

Process — Level 0

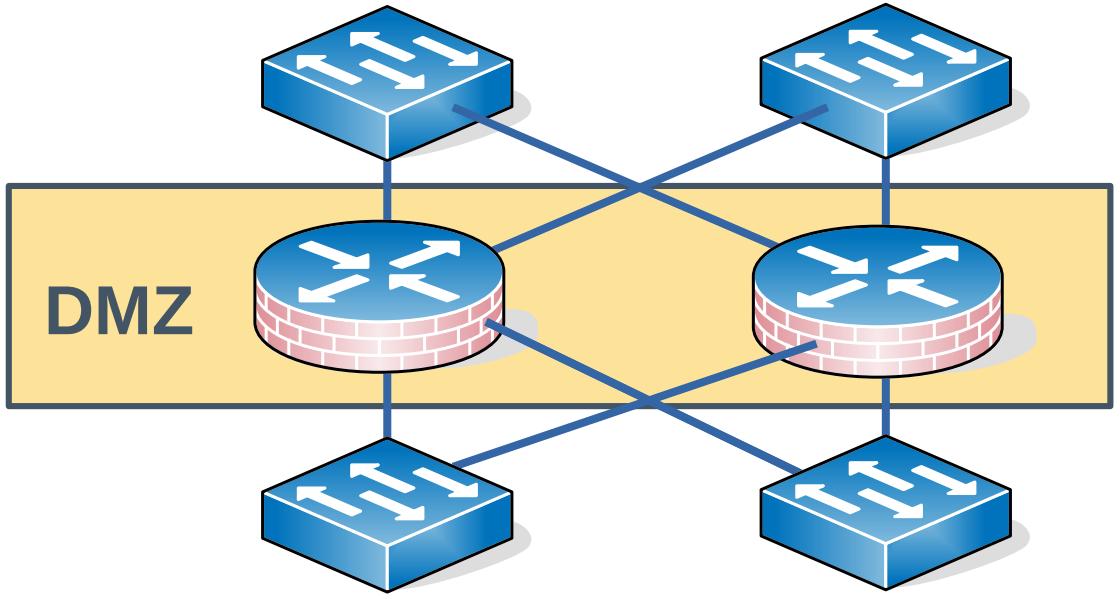
Safety Zone

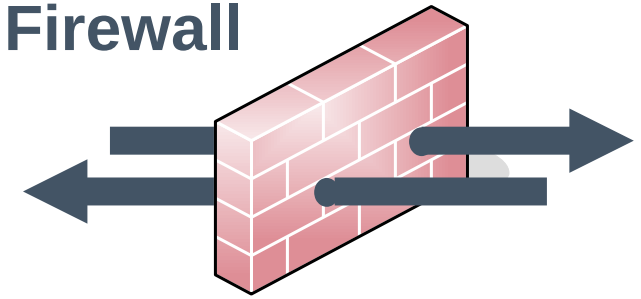
Safety-Critical

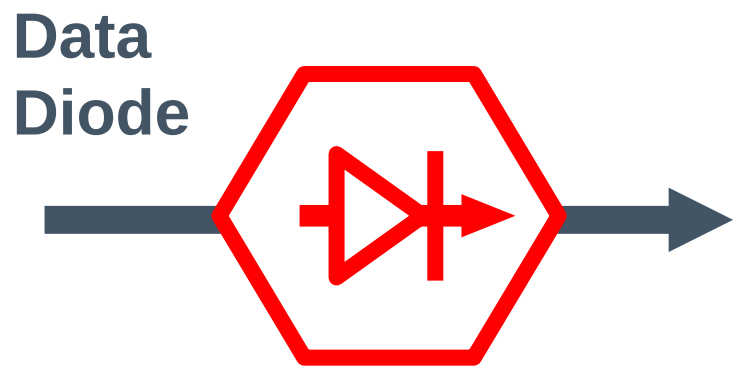
Ref: https://www.energy.gov/sites/default/files/2022-10/Infra_Topic_Paper_4-14_FINAL.pdf

Purdue Model

- **Industrial DMZ** (Level 3.5)
  - This first line of defence in isolating the IACS from IT network.







Exercise #3

Exercise #3

- **Scenario**: Take a computer parts assembly line:
  - At the end of each line there is packer **robot #1** that takes flat-packed boxes and assembles them, bends the sides, closes the 4 bottom flaps, tapes the base.
  - Another packer **robot #2** packs parts off the assembly line into the boxes and when full allows the box to continue.
  - Packer **robot #3** that inserts the manual and warranty information closes the lid, tapes the lid and affixes the product specification sticker to the box.
  - The box passes on to a sorter robot who places it in a large box along with 99 others until the large box is full, seals it and it is moved to a distribution warehouse.

Exercise #3

- **Task**: Consider that a software patch was applied to packer **robot #1** that rendered it unworkable.
  - List the consequences that you can foresee for the business, the plant and the employees if this robot is offline for two to three hours as a result.

Exercise #3

- **Business**
  - Production Slowdown, missed deadlines, production quotas not being met, and potential loss of revenue.
- **Increased Costs**
  - Overtime
  - Expedited Shipping
  - Customer Dissatisfaction
- **Plant**
  - Production Line Inefficiency
  - Inventory Buildup
  - Equipment Wear and Tear
- **Employees**
  - Downtime
  - Frustration and boredom
  - Increased Workload
  - Safety Concerns

The impact can be lessened if there are **mitigation strategies** in place.

- Part 1: OT Overview
- Part 2: Engineering a Defence

NIST Cybersecurity Framework (**CSF**) v2.0

NIST Cybersecurity Framework (CSF) v2.0

- CSF Functions

Govern (GV)

Identify (ID)

Protect (PR)

Detect (DE)

Respond (RS)

Recover (RC)

Ref: https://www.nist.gov/cyberframework

ISO 27001 ISMS

ISO/IEC 27001 – Management Requirement

- ISO/IEC 27001 provides and ISMS that allows the organisation to:
  - Systematically **identify security risks**, considering threats, vulnerabilities, and impacts.
  - Design and deploy comprehensive **security controls** or other risk treatments.
  - Maintain an ongoing process to ensure **controls remain effective**.
  - Use a coherent, **all-encompassing suite of controls**.
  - **Continuously monitor and adjust** security measures.

Ref: https://www.iso.org/standard/27001

Control Points (CP) in ISO27001:2022

Technical	• Firewalls • Intrusion detection systems • Data encryption • Password management
Organisational	• Information security policies and procedures • Training for employees • Incident response plan • Risk Assessment • Access Control • Data Security • Business Continuity
Change Management	• Offsite backup • Asset management

ISO 27001


NIST
NIST SPECIAL PUBLICATION
SP 800-82
82
Rev. 3
Guide to Operational
Technology (OT) Security
RISK MANAGEMENT FRAMEWORK

NIST SP 800-82 Rev. 3

- Guidance on how to secure OT while addressing their unique performance, reliability, and safety requirements.
- Identifies common threats and vulnerabilities to OT.
- Recommends security countermeasures to mitigate associated risks.
- Provides OT-tailored security control overlay that customises controls for the unique characteristics of the OT domain.

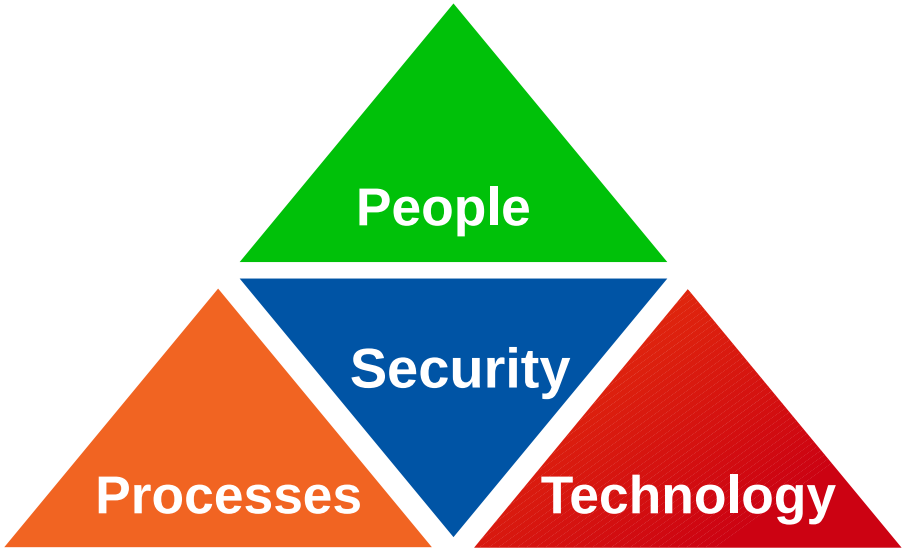
https://csrc.nist.gov/pubs/sp/800/82/r3/final

ISA/IEC 62443

Cybersecurity for operational technology in automation and control systems

ISA/IEC 62443 Series of Standards

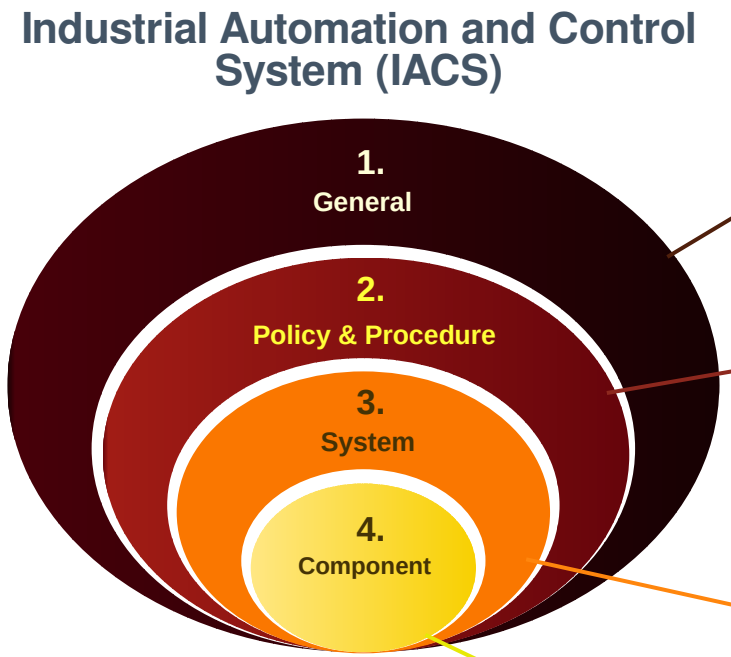
- A series of standards is a comprehensive and internationally recognised framework for securing IACS.
- It provides a holistic approach to cybersecurity, addressing all aspects of IACS security throughout their lifecycle, from design and development to operation and maintenance.



- **Core Principles**
  - Security by design
  - Security by default
  - Security throughout the lifecycle
  - Security risk management

Ref: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

ISA/IEC 62443 Series of Standards



Asset owner responsibility:

Part 1-1: Terminology, concepts and models
Part 1-2: Master glossary of terms and conditions
Part 1-3: System security conformance metrics
Part 1-4: ICAS security lifecycle and use cases

Part 2-1: Security programme requirements for IACS asset owners
Part 2-2: ICAS Security programme ratings
Part 2-3: Patch management in the IACS environment
Part 2-4: Security programme requirements for IACS service providers
Part 2-5: Implementation guidance for ICAS asset owners

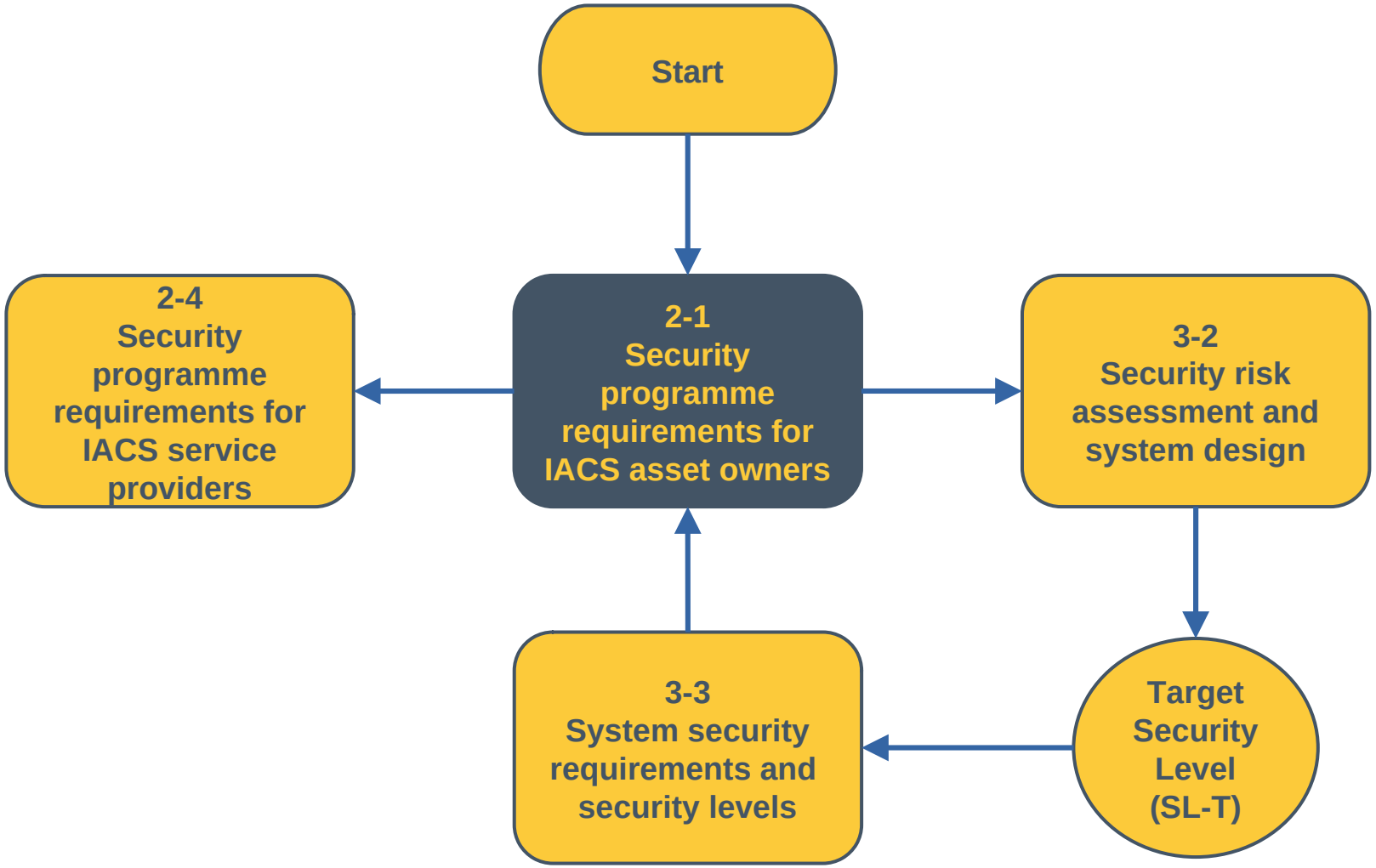
Systems Integrator responsibility:

Part 3-1: Security technologies for ICAS
Part 3-2: Security risk assessment for system design
Part 3-3: System security requirements and security levels

Component Supplier responsibility:

Part 4-1: Secure product development lifecycle requirements
Part 4-2: Technical security requirements for IACS components

ISA/IEC 62443 Relationship Between Parts



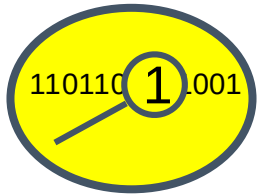

• Part 1: OT Overview
• Part 2: Engineering a Defence
• Part 3: The Adversary's Playbook

Cyber Kill Chain

What is a Kill Chain

- US Army doctrine F2T2EA, a structured procedure for identifying, engaging, and neutralising an enemy to achieve a desired outcome
  - **Find**: Locate suitable adversary targets for engagement
  - **Fix**: or pinpoint their exact location
  - **Track**: and monitor their movements
  - **Target**: Select the appropriate weapon or asset to produce the desired effects
  - **Engage**: the adversary
  - **Assess**: Evaluate the results.

Intrusion Kill Chain

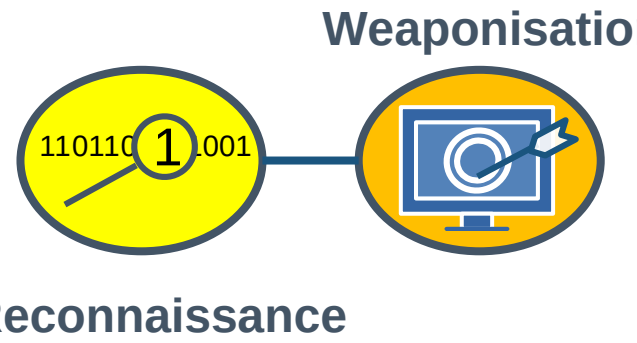


Reconnaissance

1) Reconnaissance

- Attacker gathers information about the target organisation and its systems.
- Info can be obtained from a variety of sources, such as public records, social media, and corporate websites.
- The goal is to identify vulnerabilities that the attacker can exploit to gain access to the target system.

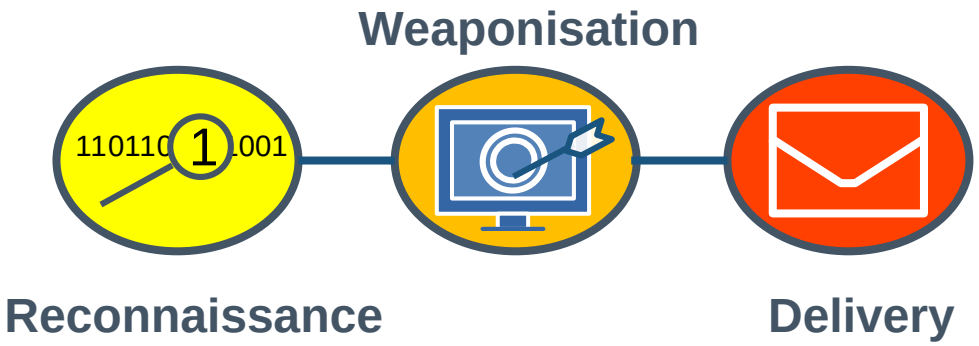
Intrusion Kill Chain



2) Weaponisation

- Develop a malicious payload.
- Code that will be used to exploit the vulnerabilities in the target system, such as a virus, worm, or Trojan horse.

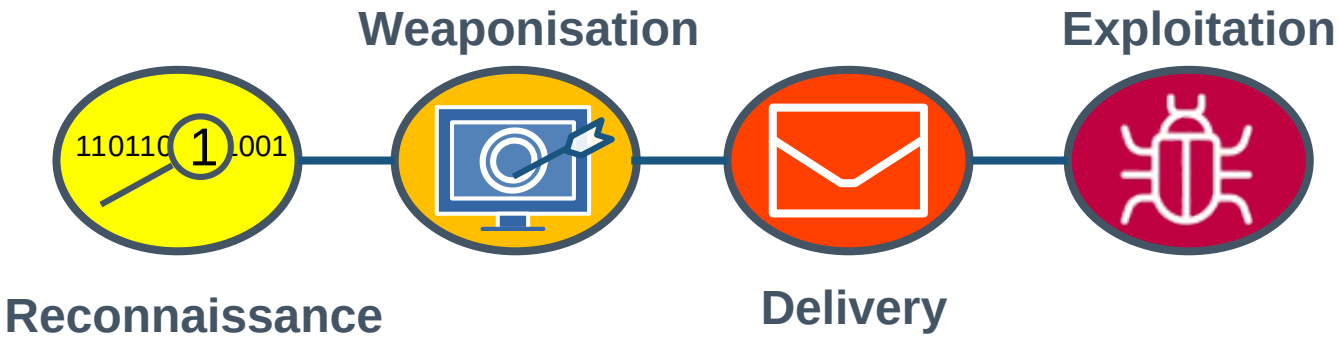
Intrusion Kill Chain



3) Delivery

- Deliver the payload to the target system,such as through email, USB drive, or network exploitation.
- Get the payload onto the target system so that it can be executed.

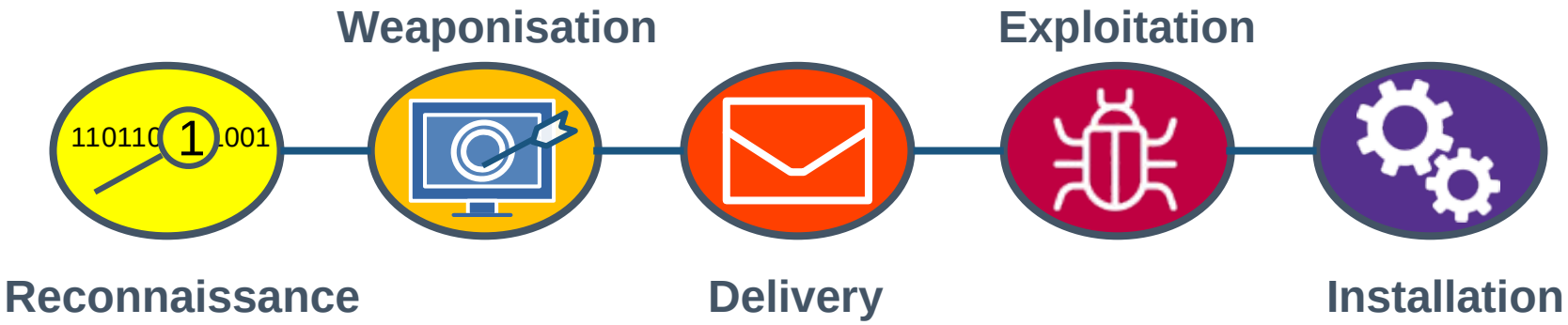
Intrusion Kill Chain



4) Exploitation

- Attempt to exploit the vulnerabilities that have been identified.
- Use the payload to execute malicious code and gain access to the system.

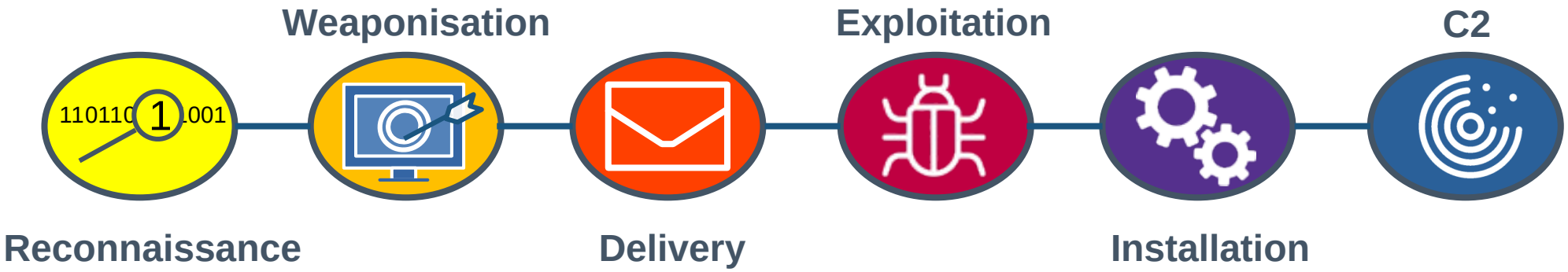
Intrusion Kill Chain



5) Installation

- Install malware or other malicious software.
- Gains control of the system to facilitate the carrying out of objectives.

Intrusion Kill Chain



6) Command and Control (C2)

- Establish a communication channel with the compromised system for remote control.
- Facilitates the stealing of data, installation of more malware, or launch other attacks.

Intrusion Kill Chain

7) Actions on Objectives

- Carry out their objectives, such as stealing data, disrupting operations, or damaging the system.

Intrusion Kill Chain

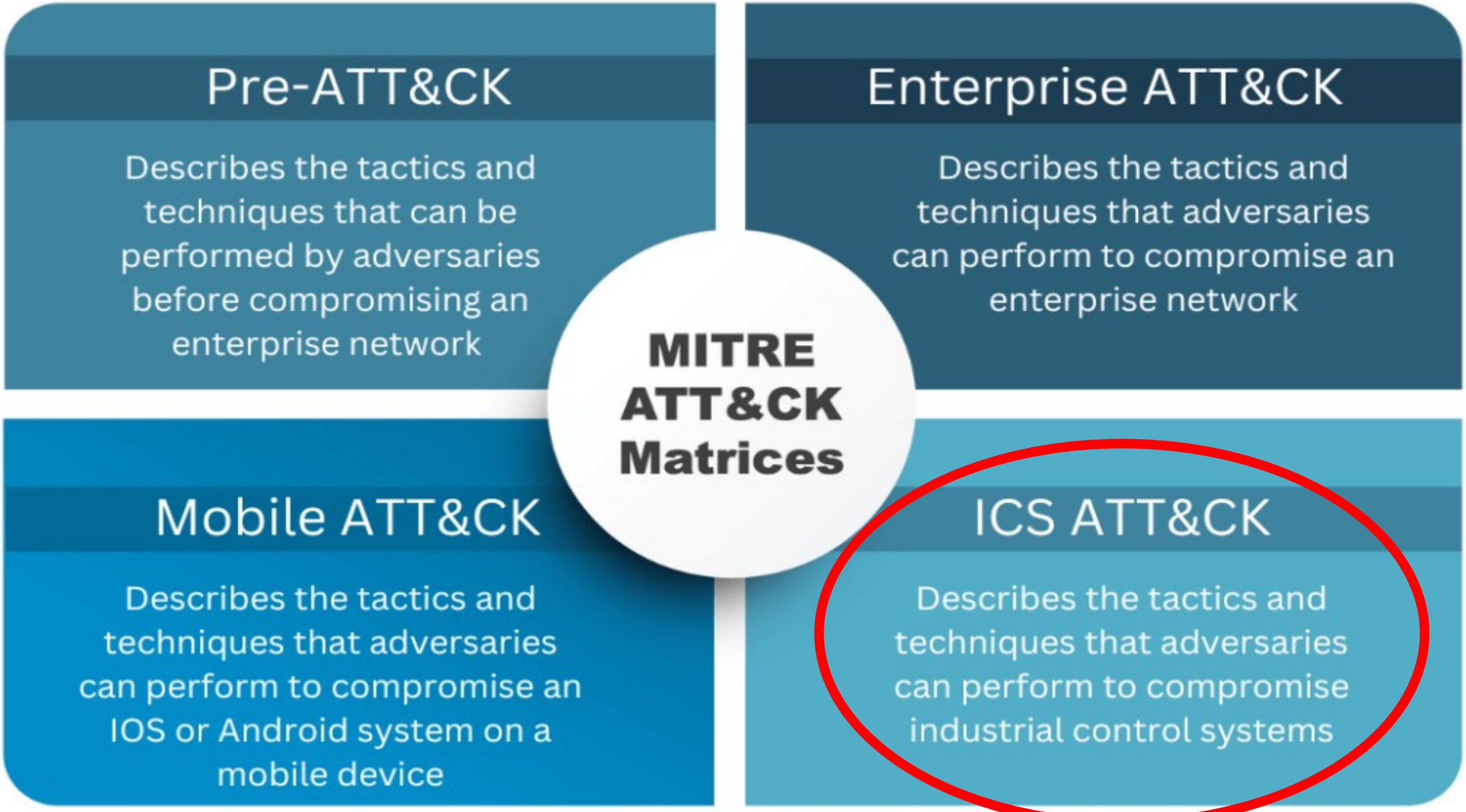
- Align defences with adversary attack processes.
- Track progress to evaluate defence effectiveness.
- Identify gaps to guide security investments.


SETU
Ollscoil
Teicneolaíochta
an Oirdheiscirt
South East
Technological
University

MITRE ATT&CK™

Introduction to MITRE frameworks

- MITRE US federally funded research organisation to solve complex national security and technical challenges since 1958.
- **ATT&CK**: a global knowledge base of real-world adversary TTPs to understand the "how" of cyberattacks developed in 2013.


Pre-ATT&CK
Describes the tactics and techniques that can be performed by adversaries before compromising an enterprise network
Enterprise ATT&CK
Describes the tactics and techniques that adversaries can perform to compromise an enterprise network
MITRE ATT&CK Matrices
Mobile ATT&CK
Describes the tactics and techniques that adversaries can perform to compromise an IOS or Android system on a mobile device
ICS ATT&CK
Describes the tactics and techniques that adversaries can perform to compromise industrial control systems

ICS Matrix

Initial Access (12 techniques)	Execution (10 techniques)	Persistence (6 techniques)	Privilege Escalation (2 techniques)	Evasion (7 techniques)	Discovery (5 techniques)	Lateral Movement (7 techniques)	Collection (11 techniques)	Command and Control (3 techniques)	Inhibit Response Function (14 techniques)	Impair Process Control (5 techniques)	Impact (12 techniques)
Drive-by Compromise	Autorun Image	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Change Operating Mode	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Command-Line Interface	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Execution through API	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Graphical User Interface	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Hooking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable Media	Modify Controller Tasking			System Binary Proxy Execution		Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Native API						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	Scripting						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise	User Execution						Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

MITRE ATT&CK™

ICS

https://attack.mitre.org/matrices/ics/

ICS Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
	10 techniques	6 techniques	2 techniques	7 techniques	5 techniques	7 techniques	11 techniques	3 techniques	14 techniques	5 techniques	12 techniques
Drive-by Compromise	Autorun Image	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Change Operating Mode	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Command-Line Interface	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Execution through API	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Graphical User Interface	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Hooking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable Media	Modify Controller Tasking			System Binary Proxy Execution		Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Native API						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	Scripting						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise	User Execution						Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

Tactics

ICS Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
	10 techniques	6 techniques	2 techniques	7 techniques	5 techniques	7 techniques	11 techniques	3 techniques	14 techniques	5 techniques	12 techniques
Drive-by Compromise	Autorun Image	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Change Operating Mode	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Command-Line Interface	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Execution through API	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Graphical User Interface	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Hooking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable media	Modify Controller Tasking			System Binary Proxy Execution		Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Native API						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	Scripting						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise	User Execution						Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

Techniques

ICS Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
	10 techniques	6 techniques	2 techniques	7 techniques	5 techniques	7 techniques	11 techniques	3 techniques	14 techniques	5 techniques	12 techniques
Drive-by Compromise	Autorun Image	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Change Operating Mode	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Command-Line Interface	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Execution through API	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Graphical User Interface	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Hooking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable media	Modify Controller Tasking			System Binary Proxy Execution		Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Native API						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	Scripting						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise	User Execution						Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

S0608 Conficker

- Exploit of Windows drive shares
- **ICS Techniques**
  - Loss of Availability
  - Loss of Productivity and Revenue
  - Replication Through Removable Media
- **ICS Mitigations**
  - Disable or Remove Feature or Program
  - Limit Hardware Installation
  - OS Configuration

Procedures & Mitigations


• Part 1: OT Overview
• Part 2: Engineering a Defence
• Part 3: The Adversary's Playbook
• Part 4: Regulation – NIS2, CII and Beyond


NIS-2

EU and Cybersecurity

- Common market, different OT Cybersecurity approaches.
- Critical National Infrastructure (CNI) risks, an incident in one member state may impact a service in another state.
- Network Information Security (NIS) Directive 2016/1148
  - Common level of security for all member states.
- Network Information Security 2 Directive 2022/2555
  - Broadened the scope of the original directive.
  - Identifies 10 sectors of high criticality and 7 other critical services.

Ref: https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng

*"**Essential**" and "**Important**" entities must take **appropriate** and **proportional** technical, operational and organisational measures to manage the risks posed to the systems.*

Three main pillars of NIS2

Member State Responsibilities

- Competent Authorities
- National Strategies
- CVD Frameworks
- Crisis Management
- Frameworks

Company Responsibilities

Risk Management

- Accountability for top management for non-compliance
- Essential and important companies are required to take security measures
- Companies are required to notify incidents within a given time frame

Co-operation and Information Exchange

- Cooperation Group
- CSIRTs Network
- CyCLONe
- CVD and European Vulnerability registry
- Peer-reviews
- Biennial ENISA cybersecurity report

Coordinated Vulnerability Disclosure (CVD)
European Cyber Crisis Liaison Organisation Network (EU-CyCLONe)
European Network Information Security Agency (ENISA)

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

*Entities may be designated as "**Essential**" or "**Important**" depending on factors such as size, sector and criticality.*

Entities

Large Enterprise

- >= 250 employees, or
- > €50m revenue

Medium Enterprise

- 50-249 employees, or
- > €10m revenue

Small & Micro Enterprise

- < 50 employees

NIS2 Sectors of high criticality

Energy

Transport

Banking

Financial Markets

Digital Infrastructure

Important Entities

Essential Entities

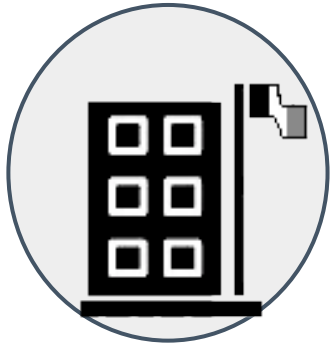
Important Entities

Drinking Water

Waste Water

Health

Space



Public Administration

Essential Entities

Important Entities

NIS2 Other critical sectors

Postal & Courier

Waste Management

Chemicals

Food

Important Entities

Essential Entities	Ex Ante
Important Entities	Ex Post

Manufacturing

Digital Providers

Research Organisations

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

*NIS2 provides NCAs with a **minimum** list of enforcement powers for non-compliance.*

NIS2 Penalties

- Strict penalties for non-compliance by entities.
- There are particularly high penalties for infringements of:
  - **Article 21 Cybersecurity risk-management measures**
  - **Article 23 Reporting obligations**
- **Essential entities** can be fined up to **€10,000,000** or at least **2%** of the total annual worldwide turnover in the previous fiscal year, whichever amount is higher.
- **Important entities** can be penalised by fines of up to **€7,000,000** or at least **1.4%** of the total annual worldwide turnover, whichever amount is higher.

National Critical Information Infrastructure Protection Centre (NCIIPC) Protected Sectors

Banking
Financial Services
Insurance

Power & Energy

Telecoms

Transport

Government

Strategic & Public Enterprises

Healthcare

NCIIPC

- NCIIPC notifies entities as “**Protected**” in the Gazette of India
- Unauthorised access to these systems is punishable by **up to 10 years** in prison.
- The organisation **must** conduct an information security audit at least once a year through a NCIIPC panelled auditor.
- A dedicated CISO must be appointed to oversee the system's resilience.

ISO/IEC 27001 ‖ ISA/IEC 62443

Indian CII Regs	ISO/IEC 27001	ISA/IEC 62443
Protected System Designation	Clause 4.3: Scope of the ISMS	62443-2-1: Establishing an IACS Security Program
CISO Appointment & Governance	Clause 5.1: Leadership & Commitment	62443-2-1: Security management & organisation
Network Segmentation	Control 8.22: Network security	62443-3-2 / 3-3: Zones, Conduits, and SL-T (Security Level-Target)
6-Hour Incident Reporting	Control 5.24: Incident management	62443-2-1 / 4-1: Incident response and lifecycle support
Cyber Crisis Management Plan	Control 5.29: Information security during disruption	62443-2-1: Business continuity and disaster recovery for IACS
Supply Chain & Trusted Sources	Control 5.19: Supplier relationships	62443-4-1 / 4-2: Secure development lifecycle and component requirements
180-Day Log Retention	Control 8.15: Logging	62443-3-3: System logging and audit trails
Vulnerability & Penetration Testing	Control 8.8: Mgmt of technical vulnerabilities	62443-2-3: Patch management and vulnerability assessment


• Part 1: OT Overview
• Part 2: Engineering a Defence
• Part 3: The Adversary's Playbook
• Part 4: Regulation – NIS2, CII and Beyond

Exercise #4
Nadu Power Grid Limited

Exercise #4 Scenario: Nadu Power Grid Ltd

- During Mattu Pongal (January 15), **Nadu Power Grid** was hit with a ransomware attack that crippled its smart-grid monitoring in Erode.
- On January 16, **Nadu Power** was contacted by an officer from **CERT-In**. The officer stated that **Bakarwal Logistics** had reported a breach on January 14. In their report, Bakarwal's CTO stated they believed the breach originated through a Site-to-Site VPN shared with **Nadu Power**'s logistics portal used for scheduling emergency grid repairs.

Exercise #4 Scenario: Nadu Power Grid Ltd

- **Nadu Power**’s IT Manager admitted they had a *minor glitch*" but didn't report it because they *restored from backups quickly to keep the lights on during the festival*. They hired **Echo Cyber** (an external firm) and spent ₹150 Lakh on restoration.

Exercise #4 Scenario: Nadu Power Grid Ltd

What jurisdiction did the CERT-In have to contact Nadu Power Grid about their incident?

2

Exercise #4 Scenario: Nadu Power Grid Ltd

What jurisdiction did the CERT-In have to contact Nadu Power Grid about their incident?

- Under the **CERT-In** Directions (April 2022), any "**Body Corporate**" (company) is legally mandated to report cyber incidents. Furthermore, if **Nadu Power** is notified as a Protected System under Section 70 of the IT Act, the NCIIPC has the mandate to intervene.
- Difference: Unlike NIS2's "**Important vs. Essential**" distinction, India's reporting mandate applies to all companies, but the severity of oversight is much higher for "**Protected Systems**."

Exercise #4 Scenario: Nadu Power Grid Ltd

Were the companies in compliance with Indian Law??

2

Exercise #4 Scenario: Nadu Power Grid Ltd

Were the companies in compliance with Indian Law??

- **Bakarwal Logistics**: **Likely In Compliance**. They reported the incident. However, they must check if they met the 6-hour mandatory reporting window (India's window is much tighter than the NIS2 24-hour warning).
- **Nadu Power**: **Non-Compliant**. By failing to report a ransomware attack (which is a specifically listed reportable incident in Annexure I of the 2022 Directions), they violated Section 70B(7) of the IT Act punishable with imprisonment for a term which may extend to one year or with fine which may extend to ₹1 lakh or with both.

Exercise #4 Scenario: Nadu Power Grid Ltd

Is there a *Case to Answer*?

2

Exercise #4 Scenario: Nadu Power Grid Ltd

Is there a *Case to Answer*?

- Reporting Obligations (Section 70B): **Nadu Power** has a clear case to answer. Failure to report to CERT-In can lead to imprisonment for up to one year or a fine up to ₹1 Lakh, though in practice, it leads to heavy regulatory scrutiny and potential license reviews.
- **Risk Management** (Protected System Rules 2018): As **Nadu Power** is a Protected System, they failed to maintain the *Point-to-Point* security standards and failed to notify the NCIIPC of a "degradation of service," which is a violation of the Information Security Practices for Protected Systems.


• Part 1: Operational Technology (OT) Overview
• Part 2: Engineering a Defence
• Part 3: The Adversary's Playbook
• Part 4: Regulation – NIS2 and Beyond
• Part 5: Wrap-up

Securing the Digital Backbone: India’s OT Framework

- **The Indian Nodal Authorities**
  - **CERT-In**: The national agency for incident response. Mandates reporting of "Cyber Security Incidents" within 6 hours of detection (IT Rules 2022/2025).
  - **NCIIPC**: Nodal agency for CII (Power, Transport, Banking, etc.) under the IT Act, 2000.
- **Sector-Specific Mandates (OT Focus)**
  - **Central Electricity Authority (CEA) Regulations 2025**, finalised guidelines for the Power Sector requiring 24/7 Information Security Divisions and mandatory audits by CERT-In panelled auditors.
  - **Digital Personal Data Protection (DPDP) Act 2023**, impacts food producers and transporters (like Nadu Power Grid) regarding the privacy of logistical and employee data.
- **The Compliance Shift**
  - Moving from "Advisory" to "Enforceable" National Cyber Security Reference Framework (NCRF 2023).
  - Emphasis on Supply Chain Security: Responsibility now extends to third-party vendors (Logistics, OEM).

Securing the Digital Backbone: India's OT Framework

- **Strengthening the Value Chain**, "*from Farm to Fork*".
- **Interdependence is reality**, an attack on a transport partner is an attack on the producer.
- **Integrating ISA/IEC 62443** is no longer optional for Indian manufacturing hubs.
- Key Action Items for the Room:
  - **Map your OT Assets**, you cannot defend what you don't see (Asset Inventory).
  - **Audit the "Air-Gap"**, ensure the Industrial DMZ (Purdue Level 3.5) actually functions.
  - **Vendor SLAs**, update contracts to include mandatory 6-hour breach disclosure.

SETU
Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

INSPIRING FUTURES

SETU
Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

EUR ING Dr Diarmuid Ó Briain
Innealtóir Cairte agus Léachtóir Sinsearach

D +353 59 917 5000 | E diarmuid.obriain@setu.ie | **setu.ie**
Campas Bhóthar Chill Chainnigh, Ceatharlach, R93 V960, Éire

SETU
Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Thank you

engcore
advancing technology