TUS

Digitalisation Leadership Bootcamp

Cyber-security in Manufacturing

Dr Diarmuid Ó Briain

Room
10A06

9 July 2024
16:00 – 17:00 hrs

Topics

- What is Operational Technology?
- The Purdue Enterprise Reference Architecture
- NIST SP 800-82 Guide to Operational Technology Security
- ISA/IEC 62443 Securing Industrial Systems
- Network Information Systems 2 (NIS-2)

What is Operational Technology (OT)?

TUS

Information Technology –v– Operational Technology

- **IT**

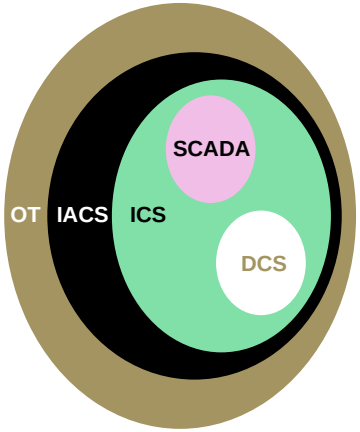
  Any equipment or interconnected system used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an organisation or by a 3rd party on the organisations behalf.

- **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)
- Industrial Automation and Control Systems (IACS)
- Industrial Control Systems (ICS)
- Supervisory Control and Data Acquisition (SCADA)
- Distributed Control System (DCS)



TUS

Exercise #1

TUS

Exercise #1

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

ESB Aghada, Cork, Ireland

TUS

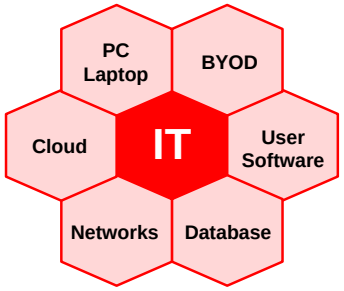
Exercise #1

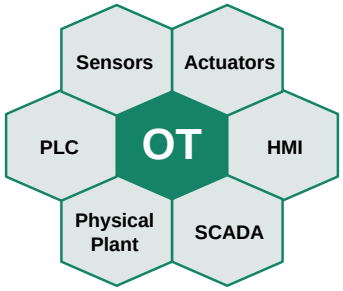
- **What is different about this power station and a typical office environment in terms of computing?**
  - Computing interacts with physical processes.
  - There is the potential for physical damage.
  - The size of such facilities and the concerns for operations and security.
  - There is a real risk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

ESB Aghada, Cork, Ireland

TUS

Information Technology -v- Operational Technology

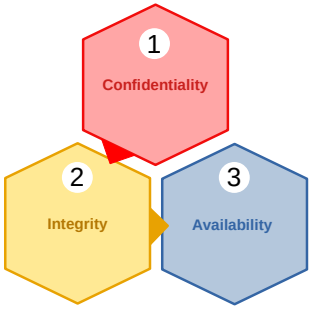




TUS

Core Principles IT/OT

IT (CIA Triad)

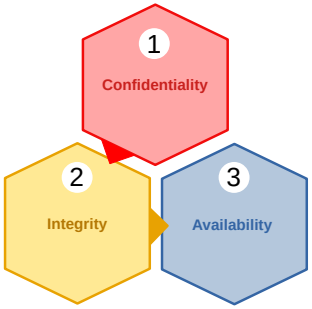


OT (SAIC)

TUS

Core Principles IT/OT

IT (CIA Triad)



OT (SAIC)

TUS

TUS

Exercise #2

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

What are the implications?

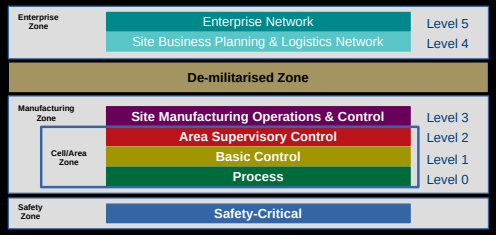
Exercise #2

- **A 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

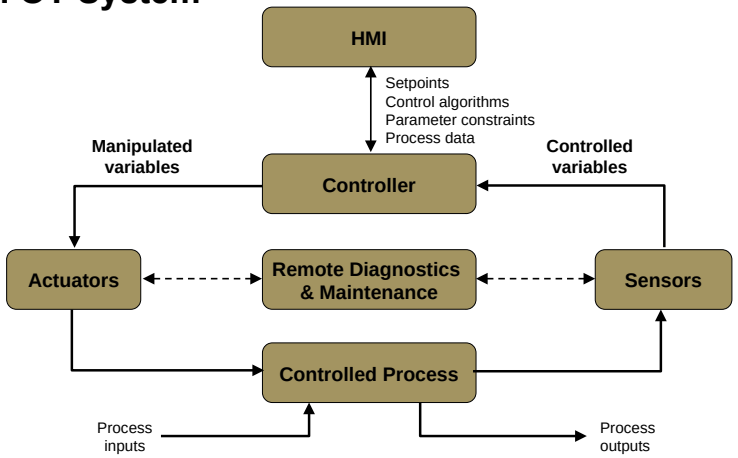
- This is why **Availability** is more important than **Confidentiality** in OT.
- Data is still very important within OT as proprietary knowledge and confidential product information can all be stored and transmitted as part of a OT network.
  - Storage of brewery recipes, process timings, security controls as well as Intellectual Property (IP).

Purdue Enterprise Reference Architecture (PERA)

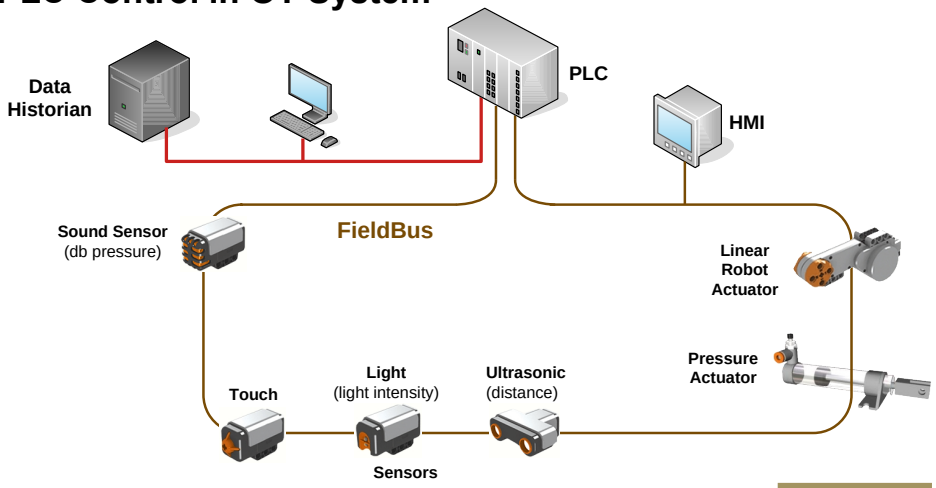


TUS

Typical OT System



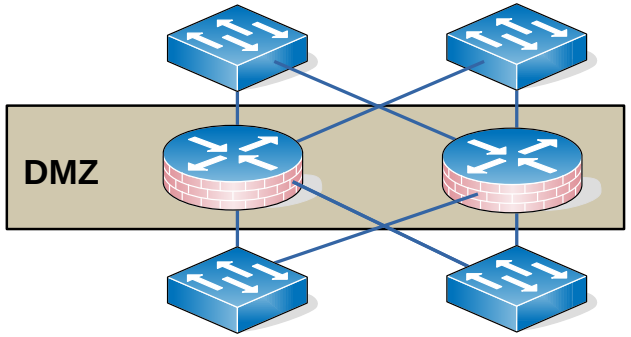
PLC Control in OT System



Functional manufacturing levels

Purdue Model

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



Data Diode

- **Firewall**
  - Rules based enforced by flexible code.
- **Data Diode**
  - Hardware one-way Ethernet connection between two networks.

TUS

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.

TUS

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.

TUS

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.

NIST SP 800-82 Rev. 3

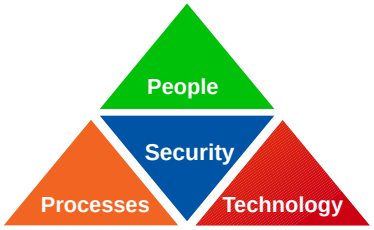
- Guidance on how to secure OT while addressing their unique performance, reliability, and safety requirements
- Identifies common threats and vulnerabilities to OT
- Recommends security countermeasures to mitigate associated risks
- Provides OT-tailored security control overlay that customises controls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

NIST SP 800-82 Rev. 3

- Establish OTSec governance
- Build and train a cross-functional team to implement an OTSec programme
- Define the OTSec strategy
- Define OT-specific policies and procedures
- Establish a OT specific cybersecurity awareness training programme
- Implement a Risk Management Framework for OT
- Develop a maintenance tracking capability
- Develop an incident response capability
- Develop a recovery and restoration capability

ISA/IEC 62443 Series of Standards

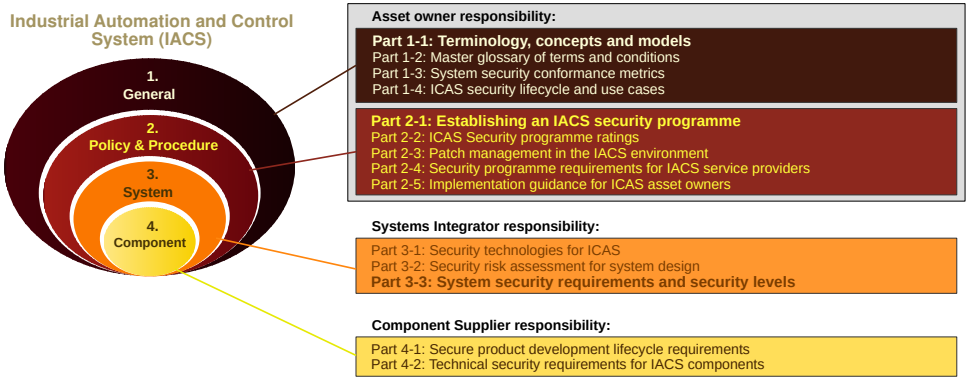
- A series of standards is a comprehensive and internationally recognised framework for securing IACS
- It provides a holistic approach to cybersecurity, addressing all aspects of IACS security throughout their lifecycle, from design and development to operation and maintenance



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

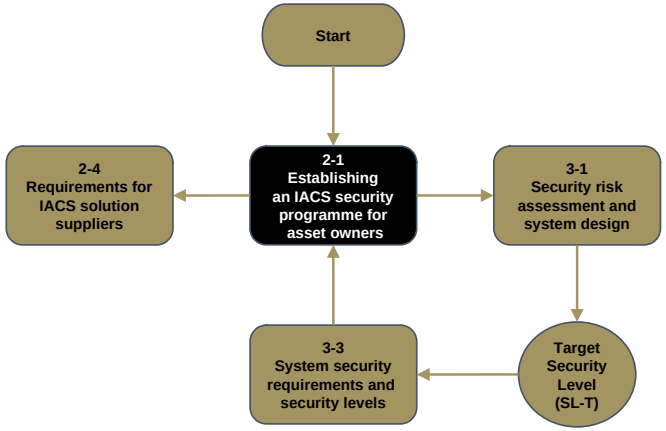
TUS

ISA/IEC 62443 Series of Standards



TUS

ISA/IEC 62443 Relationship Between Parts



TUS

NIST SP 800-82 || ISA/IEC 62443

Both the ISA/IEC 62443 and NIST SP 800-82 standards aim to improve OTSec;

- **Technical requirements**
  - **SP 800-82** provides a flexible and scalable framework for developing security controls
  - **ISA/IEC 62443** provides a detailed and prescriptive set of security controls
- **Certifications**
  - **SP 800-82** does not provide any specific certifications
  - **ISA/IEC 62443** offers a set of cybersecurity certifications for organisations
- **Flexibility**
  - **SP 800-82** standard is more flexible and can be customised to organisational needs
  - **ISA/IEC 62443** standard is more prescriptive
- **Scope**
  - **SP 800-82** is a broader framework for securing critical infrastructure systems
  - **ISA/IEC 62443** standard is specifically designed for IACS security; ISO 27001 ISMS

TUS

TUS

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.

TUS

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

TUS

Three main pillars of NIS2

Member State Responsibilities

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

Company Responsibilities

Risk Management

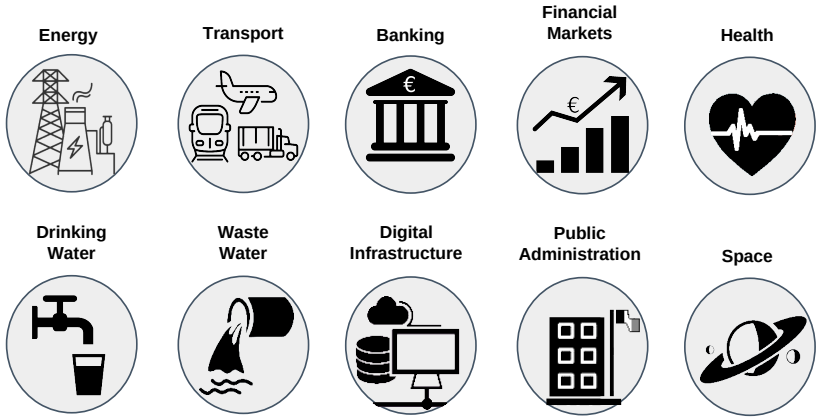
- Accountability for top management for non-compliance
- Essential and important companies are required to take security measures
- Companies are required to notify incidents within a given time frame

Co-operation and Information Exchange

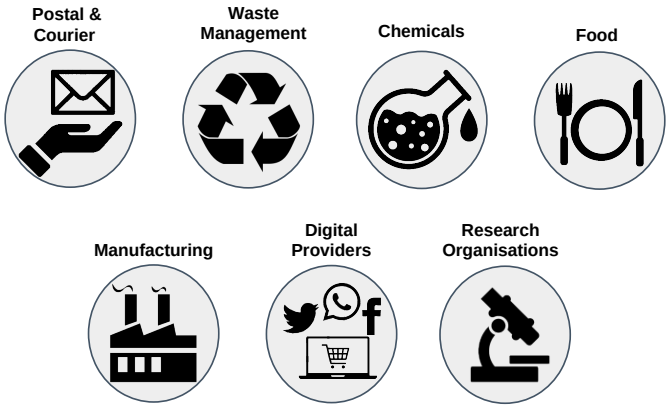
- Cooperation Group
- CSIRTs Network
- CyCLONe
- CVD and European Vulnerability registry
- Peer-reviews
- Biennial ENISA cybersecurity report

Coordinated Vulnerability Disclosure (CVD)
European Cyber Crises Liaison Organisation Network (EU-CyCLONe)
European Union Agency for Cybersecurity (ENISA)

NIS-2 Sectors of high criticality (Essential Entities)



NIS-2 Other critical sectors (Important Entities)



NIS-2 Incident Reporting obligations

Time	Incident reporting
Within 24 hours	**Early Warning** should be communicated, as well as some first presumptions regarding the kind of incident
After 72 hours	**Official Incident Notification** A full notification report must be communicated, containing the assessment of the incident, severity and impact and indicators of compromise.
Upon Request	**Intermediate Status Report** At the request of CSIRT or relevant competent authority.
After 1 month	**Final report** must be communicated.
Every 3 months	Member states CSIRT reports incidents to ENISA.
Every 6 months	ENISA reports on all incidents EU wide.

NIS-2 Penalties

- 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.

Exercise #4 Scenario: Limerick Cheeses Limited

- Saint Patrick's Day **Limerick Cheeses** was hit with a ransomware attack.
- The attack crippled its operations in Patrickswell.
- On the 1 April **Limerick Cheeses** was contacted by an officer of the NCSC who stated that **Mótar Transport** reported that they had suffered an attack and reported it on the 18 March.
- In the report the CTO of **Mótar Transport** stated that they believe the attack came through a VPN they had with **Limerick Cheeses** logistics system for processing movement orders.

Exercise #4 Scenario: Limerick Cheeses Limited

- Additionally, on the 19 March, **Mótar Transport** reported that they had to rebuild each computer on their network and restore data to their business management system from backups.
- **Limerick Cheeses** responded by stating that they did have a minor issue and that they restored their systems after working to get the systems back up as quickly as possible as the attack was disrupting their production and shipping.
- Further questioning of the IT manager at **Limerick Cheeses** revealed that they had employed the services of **Echo Cyber**, a cybersecurity firm, and the incident cost them €175,000 to get everything restored to pre-incident state.

Exercise #4 Scenario: Limerick Cheeses Limited

What jurisdiction did the NCSC have to contact Limerick Cheeses about their incident?

2

Exercise #4 Scenario: Limerick Cheeses Limited

What jurisdiction did the NCSC have to contact Limerick Cheeses about their incident?

- As a food producer ***Limerick Cheeses*** is part of a ***other critical sectors*** and they are therefore an ***important entity***.
- They are subject to ex-post supervision, meaning that as the CSIRT-IE received potential evidence of non-compliance they had the right to take action.

Exercise #4 Scenario: Limerick Cheeses Limited

Were Limerick Cheeses and Mótar Transport in compliance with the NIS2?

2

Exercise #4 Scenario: Limerick Cheeses Limited

Were Limerick Cheeses and Mótar Transport in compliance with the NIS2?

- ***Mótar Transport***, from a high criticality sector, is an essential entity, they reported the incident within 24 hours and followed up within 72 hours so they were in compliance.
- ***Limerick Cheeses*** did not report the incident, they were solicited by the NCSC because of information received from ***Mótar Transport***, so they were not in compliance.

Exercise #4 Scenario: Limerick Cheeses Limited

Is there a case to answer by either Limerick Cheeses or Mótar Transport in case of either Article 21, risk-management measures, or Article 23, reporting obligations, of the NIS2?

2

Exercise #4 Scenario: Limerick Cheeses Limited

Is there a case to answer by either Limerick Cheeses or Mótar Transport in case of either Article 21, risk-management measures, or Article 23, reporting obligations, of the NIS2?

- ***Mótar Transport***, In terms of Article 23, reporting obligations they have no case to answer; however, in the case of Article 21, Cybersecurity risk-management measures they may have.
- ***Limerick Cheeses*** infringed both Article 21 and Article 23, so they certainly have a case to answer.

Topics

- What is Operational Technology? ✓
- The Purdue Enterprise Reference Architecture ✓
- NIST SP 800-82 Guide to Operational Technology Security ✓
- ISA/IEC 62443 Securing Industrial Systems ✓
- Network Information Systems 2 (NIS-2) ✓

TUS
Ollscoil Teicneolaíochta na Sionainne
Lár Tíre, An tIarthar Láir
Technological University of the Shannon:
Midlands Midwest

EUR ING Dr Diarmuid Ó Briain
Innealtóir Cairte agus
Léachtóir Sinsearach

E diarmuid.obriain@tus.ie | W tus.ie
Campas Maoilis, Páirc Maoilis,
Luimneach, V94 EC5T, Éire

CEng, FIEI
CISSP®

Thank you

TUS