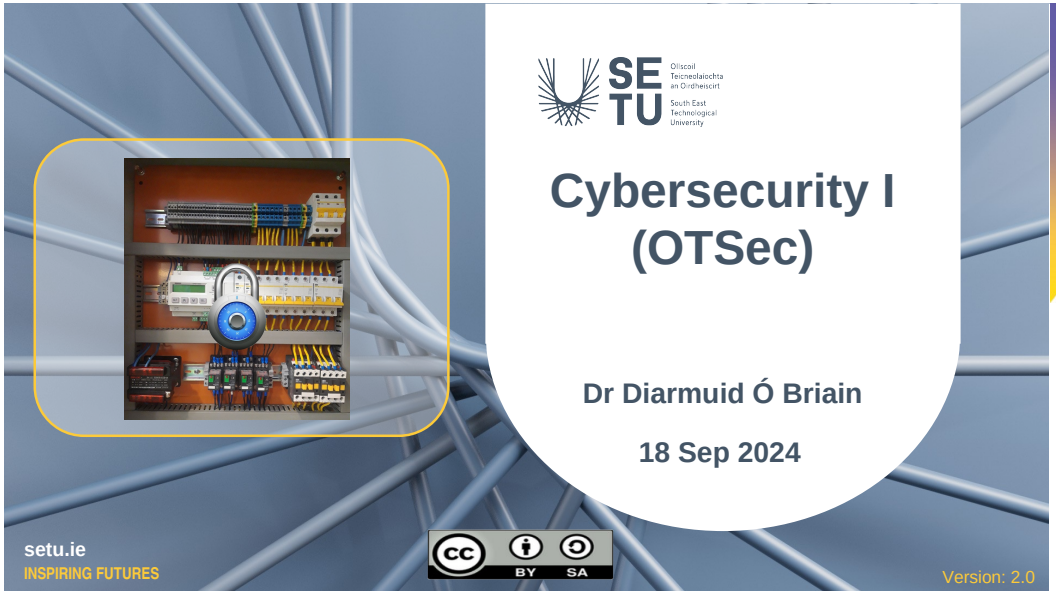


Cybersecurity I (OTSec)

Dr Diarmuid Ó Briain

18 Sep 2024

setu.ie
INSPIRING FUTURES

Version: 2.0

Licence

Module sections

- Topic 1 – Operational Technology (OT) Overview
- Topic 2 – OT Systems and Devices
- Topic 3 – Physical Security
- Topic 4 – Access Control
- Topic 5 – Frameworks
- Topic 6 – Risk Management
- Topic 7 – Incident Management
- Topic 8 – Legal Regulations Compliance and Investigations
- Topic 9 – Penetration Testing, Information gathering
- Topic 10 – Responding to a breach

Topic 1 Introduction and OT Overview

Dr Diarmuid Ó Briain

18 Sep 2024

setu.ie
INSPIRING FUTURES

Version: 2.0

Learning objectives

- At the end of this topic you will be able to:
  - Define key terms in Cybersecurity
  - Define OT
  - Define Critical Infrastructure in terms of the NIS
  - Explain the Critical Evolutions in OT
  - Consider the Security Implications of OT
  - List the differences between IT and OT
  - Explain the CIA Triad and the need to invert it for OTSec

Topic 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 cybersecurity within OT environments
  - Understands how OT supports critical infrastructure and the global need for OTSec, as it proliferates in various industries.
  - Understands that staff and public safety are the first concern when working within an industrial setting. This priority also extends to cybersecurity incident response.

Key IT and OT Security terms

IT versus OT

- 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.

IT versus OT

- 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 (IACS)
    - Building Management Systems (BMS)
    - Fire Control Systems (FCS)
    - Physical Access Control mechanisms.

Cyber Security Core Concept

- Risk Management is at the Core of Cyber Security
- As a Cyber Security Practitioner you must:
  - **Understand the Threats** to Business
  - **Identify Vulnerabilities** within the business operations and technology
  - Determine the **level of Risk** associated with these **Vulnerabilities**
  - Put in place appropriate Controls to Mitigate these risks to a level that is Acceptable to the business
- Risk Management is a **continuous** process

Asset, Vulnerability, Threat = Risk

Risk

- Risk Management
  - Risk Acceptance
  - Risk Mitigation
  - Risk Avoidance
  - Risk Transfer
- Risk Appetite
  - Mitigating Controls
  - Residual Risk

Risk Management

- Risk Assessment
  - Identify assets at risk
  - Estimate the value and severity of risk (Risk Management Policy)
  - Select controls to reduce risk

	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

	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

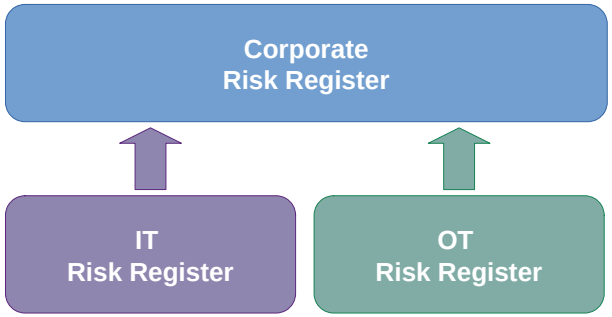
Description	Value Range
Insignificant Risk	0 - 2
Acceptable Risk	3 - 5
Unacceptable Risk	6+

Registers

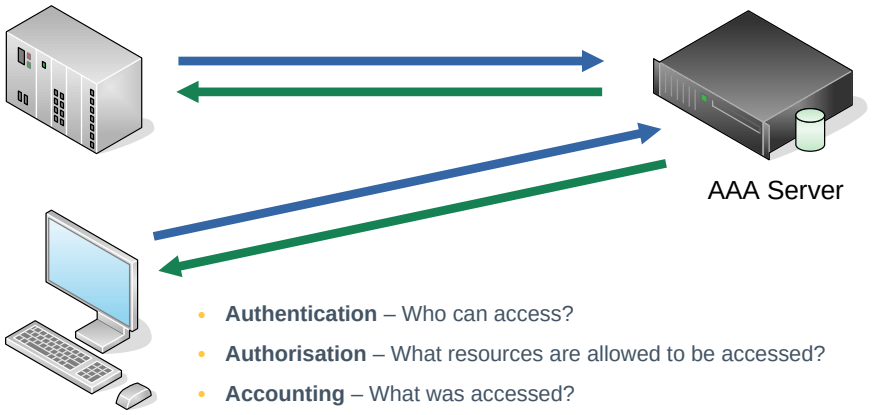
- **Corporate Risk Register**
  - *Captures, describes and assesses risks as they are identified, together with risk accountabilities, actions where required, review dates and dates when actions were completed and the risk item closed.*
- **IT Risk Register**
  - records the risks identified with ICT and IS
- **OT Risk Register**
  - records risk identified within the Industrial zone

Registers

- Risk is owned by the SMT



AAA Framework



- **Authentication** – Who can access?
- **Authorisation** – What resources are allowed to be accessed?
- **Accounting** – What was accessed?

Authentication

- **Static passwords**
- **One Time Password (OTP)**
  - PIN delivered through SMS texts or push notifications
- **Digital certificates**
  - x.509 digital certificate
- **Biometric credentials**
  - Fingerprint, Facial recognition, etc..

Authentication

- **Something you know** 332dfsak'l":@£KFede3E
- **Something you have** 
- **Something you are** 
- **Multi Factor Authentication (MFA)**

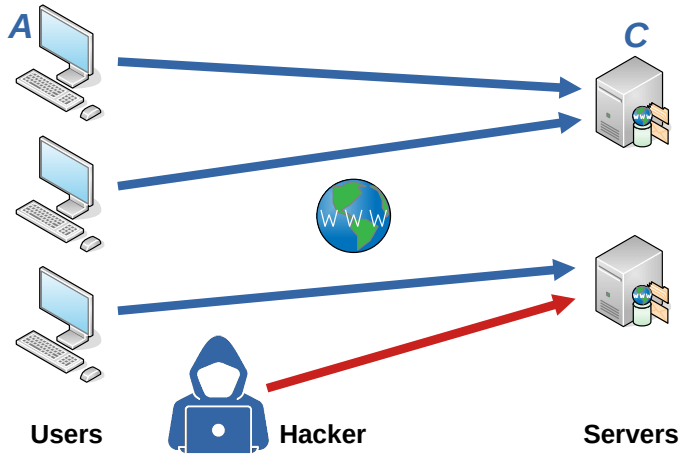
Authorisation

- *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.*

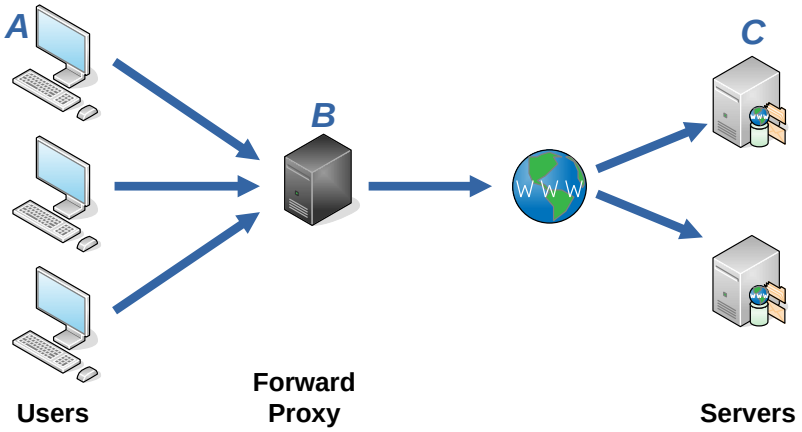
Accounting

- Keeps track of a user's activity while attached to a system;
  - Duration of time attached
  - Resources accessed
  - Volume of data transferred.
- Accounting data is used
  - Trending
  - Detecting breaches
  - Forensic investigating.

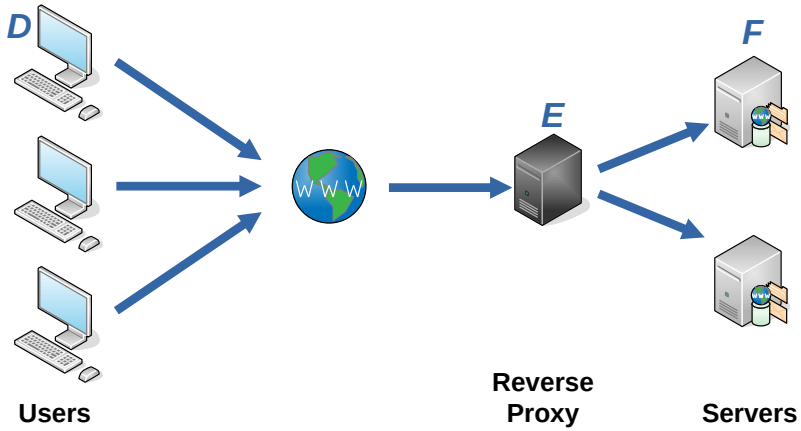
User access to resources



Proxy Server



Reverse Proxy Server

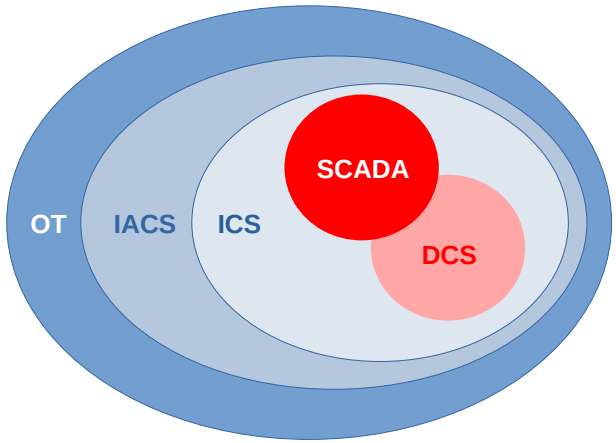


Reverse Proxy benefits

- Load Balancing
- Protection from Attacks
- Global Server Load Balancing (GSLB)
- Caching
- SSL/TLS

Introduction to Operational Technology (OT)

OT vs ICS vs IACS



Operational Technology (OT)

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

ESB Aghada, Cork, Ireland

Operational Technology (OT)

- 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.
  - There is a real risk to human life.
  - Wider implications for society if the station is disrupted.

ESB Aghada, Cork, Ireland

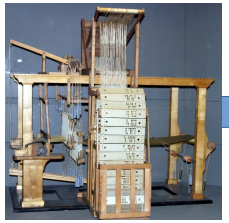
Operational Technology (OT)

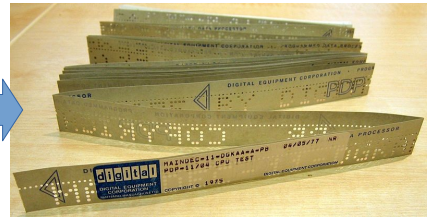
- Operational Technology are:
  - The size of such facilities and the concerns for operations and security.
  - Balancing the IT perspective and the OT perspective.
  - The paramount importance of safety concerns for health and human life.

ESB Aghada,
Cork, Ireland

Critical Evolutions in OT

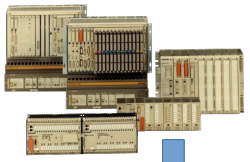
- Industrial Revolution
- Early Age of Computing
- Computing after World War 1
- Computing and Industrial Control



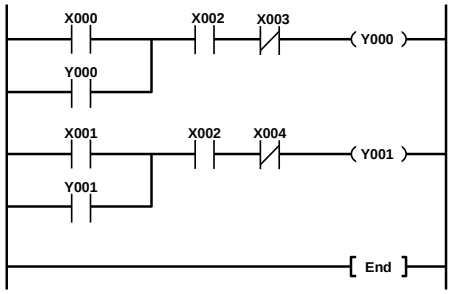


Ladder Logic

Siemens PLC Model G
(1958)



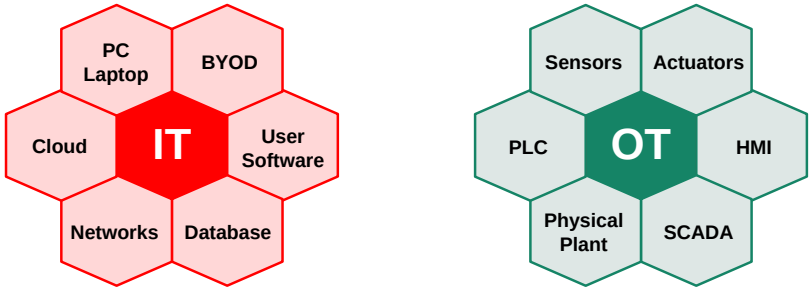
Siemens PLC s7-1500



Smart Technologies

- Smart meters roll out
- No more estimated meter readings
- Accurate energy usage data

Information Technology -v- Operational Technology



Possible incidents an OT system may face

- Blocked or delayed flow of information.
- Unauthorised changes to instructions, commands, or alarm thresholds.
- Inaccurate information sent to system operators.
- Modified OT software or configuration settings, or malware.
- Interference with the operation of equipment protection systems.
- Interference with the operation of safety systems.

Major security objectives for an OT implementation

- Restrict logical access to the OT network, network activity, and systems.
- Restrict physical access to the OT network and devices.
- Protect individual OT components from exploitation.
- Restrict unauthorised modification of data.
- Detect security events and incidents.
- Maintain functionality during adverse conditions.
- Restore the system after an incident.

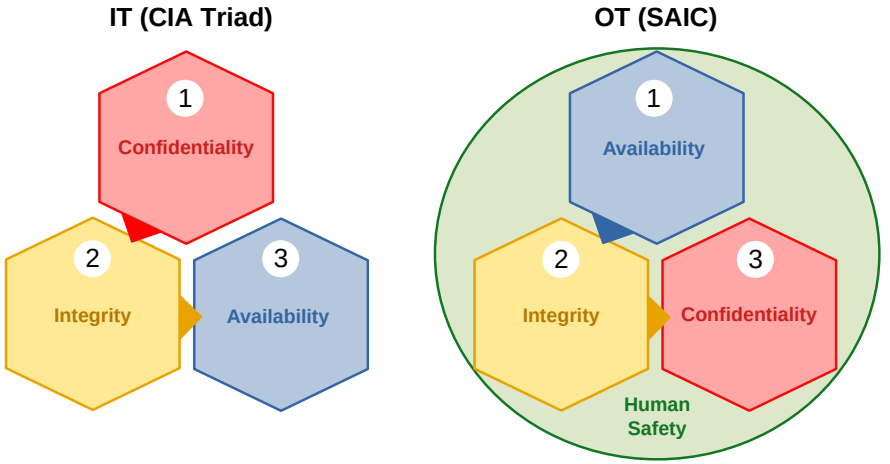
DiD Strategy should include:

1) Security policies, procedures and training.
2) Application of NCSC advisories.
3) Addressing security throughout the life cycle of the OT system.
4) Implementing a network topology for the OT system that has multiple layers.
5) Providing logical separation between the corporate and OT networks.
6) Employing a DMZ network architecture.
7) Ensuring redundancy for critical components.
8) Designing critical systems for graceful degradation.
9) Disabling unused ports and services.
10) Restricting physical access to the OT network and devices.

DiD Strategy should include:

11) Restricting OT user based on the principle of least privilege.
12) Separate authentication mechanisms and accounts for users on OT/IT.
13) Using modern technology, such as smart cards for user authentication.
14) Security controls such as intrusion detection software, antivirus software, etc....
15) Apply encryption/cryptographic hashes to OT data storage and communications.
16) Deploying security patches 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.

Core principles of information security



Example

Example

- 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?

Example

- 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 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.

What does this demonstrate?

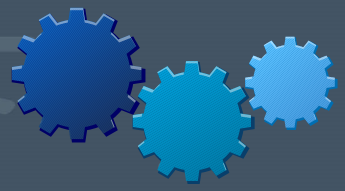
Example

- 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.
  - In a 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.

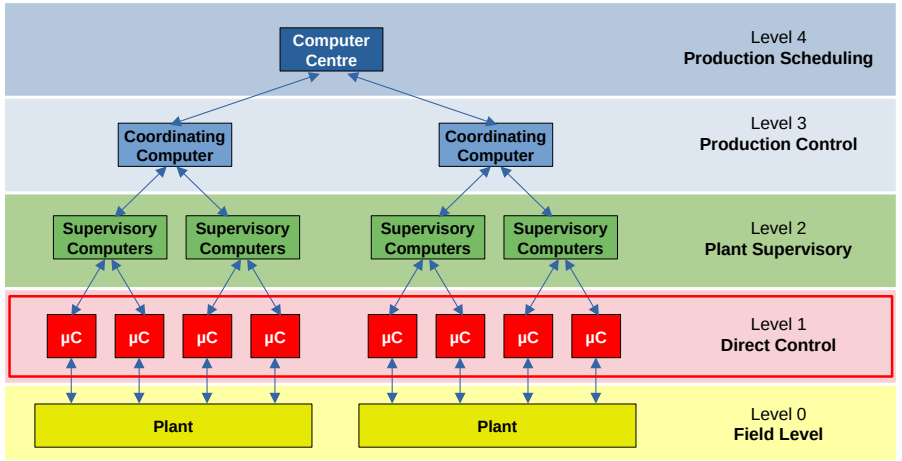
Exercise #1

Ollscoil Teicneolaíochta an Oirdheisceirt
South East Technological University

Scenario



Functional manufacturing levels



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 that are required

D) All of the above

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 that are required

D) **All of the above** ✓

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

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

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

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

Managing Risk in IT and OT

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

A) Protect Assets and Reduce Risk
B) Protect Revenue while maintaining Operational Availability
C) Which of these would be another way to describe the Enterprise Risk Management cycle?
D) Measure the risks and Control them, then see where you can improve your process
E) Find the potential risks, measure those risks, set acceptable limits for the risk, review and re-examine those limits, then repeat
F) Find the potential risks, then control them, then assess them, after that you can relax a bit
G) Control risk at all times and in all situations, then measure it, then review that measurement and then find possible risks

Managing Risk in IT and OT

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

A) Protect Assets and Reduce Risk
B) **Protect Revenue while maintaining Operational Availability** ✓
C) Which of these would be another way to describe the Enterprise Risk Management cycle?
D) Measure the risks and Control them, then see where you can improve your process
E) Find the potential risks, measure those risks, set acceptable limits for the risk, review and re-examine those limits, then repeat
F) **Find the potential risks, then control them, then assess them, after that you can relax a bit** ✓
G) Control risk at all times and in all situations, then measure it, then review that measurement and then find possible risks

Learning outcomes

You should now be able to:

- Define key terms in Cybersecurity ✓
- Define OT ✓
- Define Critical Infrastructure in terms of the NIS ✓
- Explain the Critical Evolutions in OT ✓
- Consider the Security Implications of OT ✓
- List the differences between IT and OT ✓
- Explain the need to invert the CIA Triad for Industrial Security ✓

TUS
Ollscoil Teicneolaíochta na Sionainne: Lár Tíre, An Iarthar 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