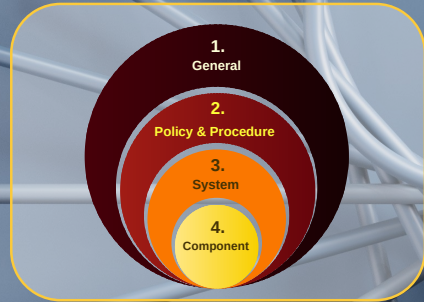


Topic 4.1 ISA/IEC 62443

Dr Diarmuid Ó Briain

11 Mar 2025



Licence



This work is licensed under a Creative Commons
Attribution-ShareAlike 4.0 International License.
Full License: <http://creativecommons.org/licenses/by-sa/4.0>

Learning objectives

At the end of this section of the topic on ISA/IEC 62443 the learning will:

- understand the importance of securing IACS and the unique challenges they face compared to IT systems.
- gain a thorough understanding of the Purdue model, a widely recognised framework for classifying and securing IACS environments.
- appreciate the key principles and structure of the ISA/IEC 62443 standard, a comprehensive framework for industrial cybersecurity.
- identify and apply the foundational requirements, terminology, and concepts outlined in the ISA/IEC 62443 Part 1: General standard.

Why Secure IACS

The consequences of a cyberattack on an IACS include:

- Endangerment of public or employee safety or health
- Damage to the environment
- Damage to the EUC
- Loss of product integrity
- Loss of public confidence or company reputation
- Violation of legal or regulatory requirements
- Loss of proprietary or confidential information
- Financial loss
- Impact on entity, local, state, or national security.

Security Objective

Security Objective	Priority
Safety	Overarching
Availability	Highest
Integrity	High
Confidentiality	Medium
Accessibility	Lowest

How are IACS different from IT Systems?

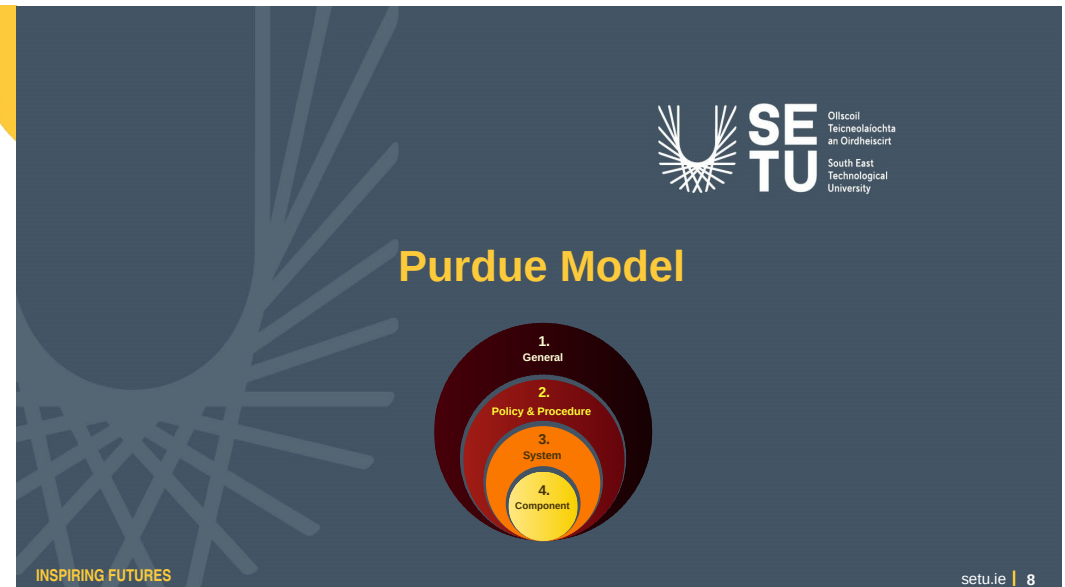
Cybersecurity in OT must be approached in the context of:

- More predictable failure modes
- Tighter time-criticality and Determinism
- Higher Availability
- More rigorous change management
- Longer time periods between maintenance lifecycles
- Significantly longer component life
- SAICA instead of the CIA triad.

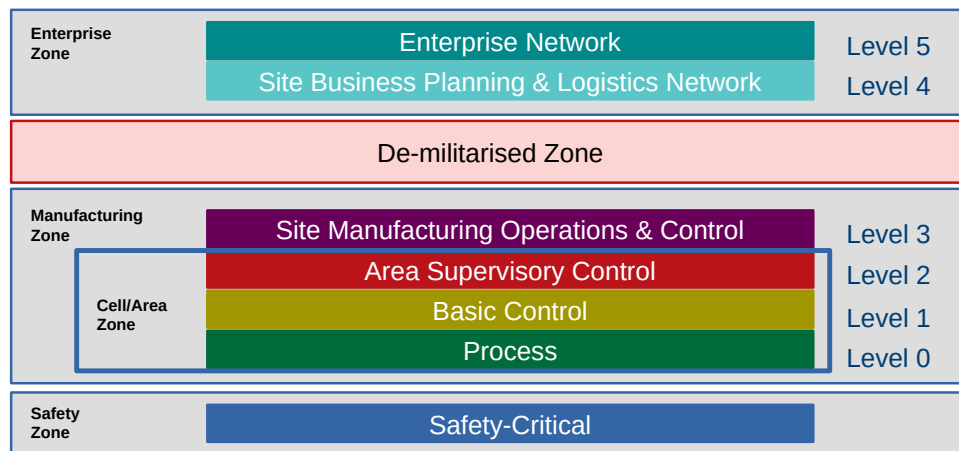
How to Secure IACS

Implementation of procedures and creating policies and processes over the following basic steps:

- Execute a Risk Assessment
- Consider each risk in terms of Security Level
- Use Maturity Levels to measure how thoroughly requirements are met
- Careful application of Cybersecurity Design Principles



Purdue Model

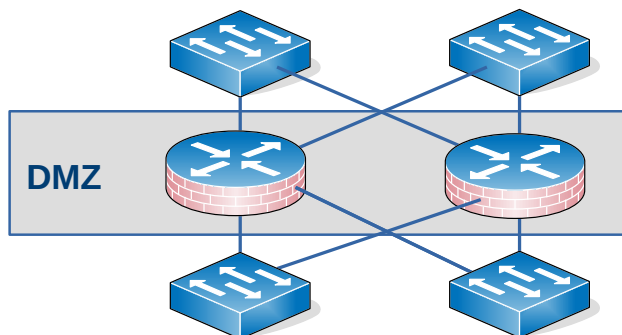


Enterprise Zone

- **Enterprise network (Level 5)**
 - Corporate level IT systems that span multiple facilities or plants
 - Store and manipulate data from subordinate systems from individual plants and use the accumulated data to report on the overall production status, inventory, and demand
 - Technically not part of the IACS.
- **Site business planning and logistics (Level 4)**
 - IT systems that support the production process in a plant of a facility
 - Systems to report production statistics such as uptime and units produced for corporate systems and take orders and business data from the corporate systems to be distributed among the ICS systems.

Purdue Model

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



Data Diode

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



Manufacturing Zone

- **Site Operations (Level 3)**

- Systems that support plant wide control and monitoring functions reside
- HMI systems to perform tasks such as quality control checks, managing uptime, and monitoring alarms, events, and trends
- Systems reporting, upwards, to IT systems in level 4
- Lower level production data is collected and aggregated by servers in this level
- Systems such as database servers, application servers, file servers, Domain controllers, HMI servers and engineering workstations.

Cell Zone

- **Area Supervisory Control (Level 2)**

- Each functional cell or production line within the ICS network is further segmented
- Placing Firewalls at strategic points within the ICS network to granularly segment different zones
- This creates an extra layer of protection for the devices, and protects the data flow and communications between them.

Cell Zone

- **Basic Control (Level 1)**

- Devices in this level is to open valves, move actuators, start motors

- **Process (Level 0)**

- EUC, process equipment being controlled and monitored from the higher levels such as motors, pumps, valves, and sensors that measure speed, temperature, or pressure
- The actual process is performed and where the product is made, it is imperative that things run smoothly and uninterrupted.

Exercise #1



Exercise #1

- **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 #1

- **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.



ISA/IEC 62443
Cybersecurity for operational technology in automation and control systems

ISA/IEC 62443 Standard

- 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.

ISA/IEC 62443 Core Principles

- Security by design
- Security by default
- Security throughout the lifecycle
- Security risk management

ISA/IEC 62443 four parts

Part 1: General

- **Part 1-1:** Terminology, concepts and models
- **Part 1-2:** Master glossary of terms and abbreviations
- **Part 1-3:** Security system conformance metrics
- **Part 1-4:** IACS security lifecycle and use cases
- **Part 1-5:** Scheme for ISA62443 security profiles

Part 2: Policies and Procedures

- **Part 2-1:** Establishing an IACS security programme
- **Part 2-2:** IACS security protection 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 IACS asset owners

ISA/IEC 62443 Six parts

Part 3: System

Part 3-1: Security Technologies for IACS

Part 3-2: Security risk assessment for system design

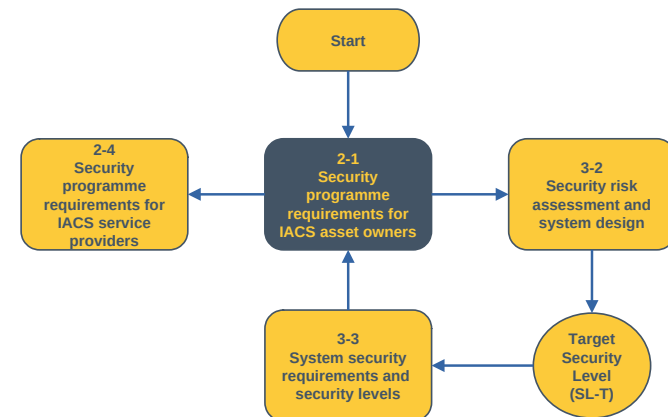
Part 3-3: System security requirements and security levels

Part 4: Component

Part 4-1: Secure product development lifecycle requirements

Part 4-2: Technical security requirements for IACS components

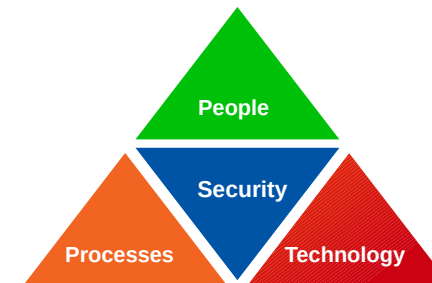
ISA/IEC 62443 relationship between parts



Benefits of ISA/IEC 62443

- Reduced risk of cyber attacks
- Improved resilience
- Enhanced compliance
- Improved operational efficiency
- Reduced costs

Scope of ISA/IEC 62443



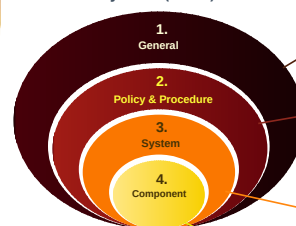
- Design and Maintenance
 - Processes, People
- Product Development
 - Processes, People, Technology

Key Roles

- **The Asset Owner:** is the organisation that has the ultimate responsibility for the security of its IACS.
- **Maintenance Service Provider:** is responsible for maintaining and supporting the IACS.
- **Integration Service Provider:** is responsible for integrating new or upgraded IACS components into the existing infrastructure.
- **Product Supplier:** is responsible for designing, developing, manufacturing, and supporting the IACS components.
- These roles are not mutually exclusive, and the responsibilities can be shared between different organisations.
 - For example, the asset owner may contract out the maintenance and integration services to third parties.

ISA/IEC 62443 Series

Industrial Automation and Control System (IACS)



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 Part 1: General

Industrial Automation and Control System (IACS)



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 1-1: Terminology, Concepts, and Models

- Core concepts
- Security domains
- Security functions
- Security assurance

Part 1-1: Concepts

The ISA/IEC 62443-1-1 important concepts include:

- Operational Technology (OT)
- Information Technology (IT)
- Cyber-physical systems (CPS)
- Attack surface
- Vulnerability
- Risk
- Security posture
- Security programme

Part 1-1: Models

The ISA/IEC 62443-1-1 several models including:

- Security zone model
- Security architecture model
- Security risk management model
- Compliance model

Foundational Requirements (FR)

- Form the basis for technical requirements throughout the ISA/IEC 62443 series of standards.
- All aspects associated with meeting a desired IACS security level (people, processes, and technology) are derived through meeting the requirements associated with the seven following FRs:
 - FR 1 – Identification and Authentication Control (IAC)
 - FR 2 – User Control (UC)
 - FR 3 – System Integrity (SI)
 - FR 4 – Data Confidentiality (DC)
 - FR 5 – Restricted Data Flow (RDF)
 - FR 6 – Timely Response to Events (TRE)
 - FR 7 – Resource Availability (RA)

FR 1 – Identification & Authentication Control (IAC)

- **Rationale:** Asset owners must develop a list of valid users (Humans, software processes and devices) as well as the required level of identification and authentication for each zone.
- **Goal:** is to protect the IACS from unauthenticated access by verifying the identity of any user requesting access to the IACS before activating the communication.

FR 1 – Security Requirements

- SR 1.1 User Identification and Authentication
- SR 1.1 RE-2 Multi-factor Authentication
- SR 1.2 Software process and device identification and authentication
- SR 1.3 Account management
- SR 1.4 Identifier management
- SR 1.5 Authenticator management
- SR 1.6 Wireless access management
- SR 1.7 Strength of password- based authentication

FR 1 – Security Requirements

- SR 1.10 Authenticator feedback
- SR 1.11 Unsuccessful login attempts
- SR 1.12 System use notification
- SR 1.13 Access via untrusted networks
- SR 1.13 RE-1 Explicit access request approval

FR 2 – User Control (UC)

- **Rationale:** Once user is authenticated, the control system has to restrict the allowed actions to the authorised use of control system. Asset owners will have to assign privileges to each user (human, software and process), group, role, etc.
- **Goal:** is to protect against unauthorised actions on IACS resources by verifying necessary privileges.
- **Privileges:** Reading, Writing, Downloading programs, setting configurations, User privileges may vary based on location, time and means of access.

FR 2 – Security Requirements

- SR 2.1 Authorisation enforcement
- SR 2.2 Wireless use control
- SR 2.3 Use control for portable and mobile device
- SR 2.4 Mobile code
- SR 2.5 Session lock
- SR 2.6 Remote session termination
- SR 2.8 Auditable events
- SR 2.9 Audit storage capacity
- SR 2.10 Response to audit processing failures
- SR 2.11 Timestamps

FR 3 – System Integrity (SI)

- **Rationale:** Asset owners are responsible for maintaining the integrity of the IACS and they may assign different levels of integrity protection to different systems, communication channels and information.
- **Goal:** The integrity of logical assets should be maintained while in transit and at rest, such as being transmitted over a network or when residing in a data repository.

FR 3 – Security Requirements

- SR 3.1 Communication integrity
- SR 3.1 RE-1 Cryptographic integrity protection
- SR 3.2 Malicious code protection
- SR 3.2 RE-1 Malicious code protection on entry and exit points
- SR 3.3 Security functionality verification
- SR 3.4 Software and information integrity
- SR 3.5 Input Validation

FR 3 – Security Requirements

- SR 3.6 Deterministic Output
- SR 3.8 Session integrity
- SR 3.8 RE-1 Invalidation of session IDs after session termination
- SR 3.8 RE-2 Unique session ID generation
- SR 3.10 Support for updates
- SR 3.14 Integrity of the boot process

FR 4 – Data Confidentiality (DC)

- **Rationale:** To prevent unauthorised disclosure IACS shall provide the necessary capabilities to ensure the confidentiality of information.
- **Goal:** Communication channels and data storages need to be secured whether at rest or in motion.

FR 4 – Security Requirements

- SR 4.1 Information confidentiality
- SR 4.3 Use of cryptography

FR 5 – Restricted Data Flow (RDF)

- **Rationale:** Asset owners need to determine necessary information flow restrictions and determine the configuration of the conduits used to deliver this information. The IACS shall provide necessary capabilities to segment the control system via zones and conduits to limit unnecessary data flow.
- **Goal:** Mechanisms such as disconnecting business networks from business or public networks by using data diodes, firewalls and creation of Demilitarised zones.

FR 5 – Security Requirements

- SR 5.1 Network segmentation
- SR 5.1 RE-1 Physical Network segmentation
- SR 5.2 Zone boundary protection
- SR 5.2 RE-1 Deny by default, allow by exception
- SR 5.2 RE-2 Island mode
- SR 5.3 General purpose person-to-person communication restrictions
- SR 5.4 Application partitioning

FR 6 – Timely Response to Events (TRE)

- **Rationale:** Asset owners shall establish security policies and procedures and proper lines of communication and control needed to respond to security violations.
- **Goal:** Use of monitoring tools and techniques should not interfere with control system and thus not degrade the performance of the system.

FR 6 – Security Requirements

- SR 6.1 Audit log accessibility

FR 7 – Resource Availability (RA)

- **Rationale:** To ensure that the control system is resilient to various types of resource consuming attacks such as Denial of Service (DoS) and to prevent partial or total unavailability of system.
- **Goal:** Use of redundant network to provide high availability at network level and high availability servers, firewalls or application level redundancy.

FR 7 – Security Requirements

- SR 7.1 DoS protection
- SR 7.2 Resource management
- SR 7.3 Control system backup
- SR 7.4 Control system recovery and reconstitution
- SR 7.5 Emergency power
- SR 7.6 Network and security configuration settings
- SR 7.7 Least functionality

Part 1-2: Master Glossary of Terms and Conditions

- This standard provides a glossary of terms or definitions of IACS related terminology that is used throughout the standard.
- The glossary is not a stand-alone document and should be used in conjunction with the standard to fully understand its requirements and terminology.

Part 1-3: System Security Conformance Metrics

The **Metrics and Measurements** are grouped into the following categories:

- Asset security metrics
- Communication security metrics
- Application security metrics
- Operational security metrics

Part 1-3: System Security Conformance Metrics

The **Measurement Approach** methodology include the following steps:

- Data collection
- Data analysis
- Action planning
- Monitoring and improvement

Part 1-4: IACS Security Lifecycle

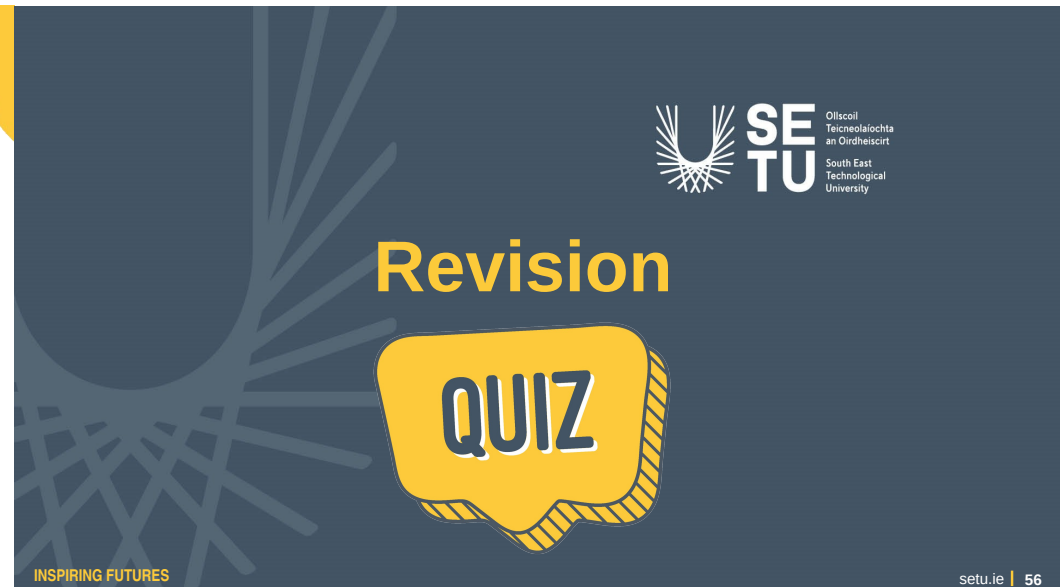
- Design
- Implementation
- Operation
- Retirement

Part 1-4: IACS Use Cases

- Defending against cyber attacks
- Protecting against data breaches
- Enhancing system availability
- Mitigating operational safety risks

Part 1-4: IACS Key Requirements

- Security by design
- Security by default
- Security throughout the lifecycle
- Security risk management

A graphic with a dark blue background featuring a stylized sunburst pattern. In the top right corner is the SE TU logo with the text 'Ollscoil Teicneolaíochta an Oirdheiscirt' and 'South East Technological University'. The word 'Revision' is written in large, bold, yellow letters. Below it, the word 'QUIZ' is written in white letters inside a yellow speech bubble with a striped border. At the bottom left, the text 'INSPIRING FUTURES' is visible.

SE TU
Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Revision

QUIZ

INSPIRING FUTURES

Question 1

- Which one SR doesn't belong to Use Control (UC)?

- ☐ Password Strength
- ☐ Authentication Enforcement
- ☐ Remote System Termination
- ☐ Response to audit processing failures

Question 1

- Which one SR doesn't belong to Use Control (UC)?

- ☒ Password Strength
- ☒ Authentication Enforcement
- ☒ Remote System Termination
- ☒ Response to audit processing failures

Question 2

- Which one SR belongs to Timely Response to Events (TRE)?

- ☐ Resource Management
- ☐ Authentication Enforcement
- ☐ Audit log Accessibility
- ☐ Restricted Data Flow

Question 2

- Which one SR belongs to Timely Response to Events (TRE)?

- ☒ Resource Management
- ☒ Authentication Enforcement
- ☒ Audit log Accessibility
- ☒ Restricted Data Flow

Question 3

- Which SRs belongs to System Integrity (SI)?

- ☐ Cryptographic integrity protection
- ☐ Security functionality verification
- ☐ Audit log Accessibility
- ☐ Input Validation

Question 3

- Which SRs belongs to System Integrity (SI)?

- ☒ Cryptographic integrity protection
- ☒ Security functionality verification
- ☒ Audit log Accessibility
- ☒ Input Validation



Question 4

- The goal of Identification and Authentication Control (IAC) is to

- ☐ protect against unauthorised actions on IACS resources by verifying necessary privileges.
- ☐ protect the IACS from unauthenticated access by verifying the identity of any user requesting access to the IACS before activating the communication.
- ☐ communication channels and data storages need to be secured whether at rest or in motion.
- ☐ use of monitoring tools and techniques should not interfere with control system and thus not degrade the performance of the system.

Question 4

- The goal of Identification and Authentication Control (IAC) is to

- ☒ protect against unauthorised actions on IACS resources by verifying necessary privileges.
- ☒ protect the IACS from unauthenticated access by verifying the identity of any user requesting access to the IACS before activating the communication.
- ☒ communication channels and data storages need to be secured whether at rest or in motion.
- ☒ use of monitoring tools and techniques should not interfere with control system and thus not degrade the performance of the system.



Laboratory #1



Risk Assessment of Location Alpha (U101) for WindPower Limited

- Part 1 – Risk Assessment Briefing



Introduction

- Location Alpha (U101) is a key component of the WindPower's electrical utility operations, responsible for generating and distributing electricity to homes and businesses across Ireland.
- This assessment will focus on evaluating U101's performance and identifying areas for improvement within the context of cybersecurity standards.

Scope

The scope of this assessment includes:

- **System Architecture:** Understanding the overall layout and interconnectivity of U101's power generation and distribution systems, including its connection to other power plants and distribution networks.
- **Asset Inventory Details:** Reviewing U101's asset management practices, including tracking of maintenance supplies, and spare parts.
- **Cybersecurity Practices:** Assess the cybersecurity practices in terms of the WindPower Limited security posture.

Assessment Objectives

The primary objectives of this assessment are to:

- Assess U101's overall cybersecurity efficiency and effectiveness compared to WindPower standards.
- Identify areas where U101's operations could be optimised to improve cybersecurity efficiency, reduce costs, and enhance reliability.
- Evaluate U101's asset management practices and make recommendations for improvement.

Assessment Methodology

As a class brainstorm assessment methodologies, how will the assessment be conducted?



Assessment Methodology

The assessment will utilise a combination of methods, including:

- **Document review:** Thoroughly reviewing relevant documentation, including system architecture diagrams, inventory control procedures, and energy consumption reports.
- **Site visits:** Conducting site visits to U101 to gain a first-hand understanding of the plant's operations, infrastructure, and equipment.
- **Interviews:** Engaging with plant personnel, including engineers, operators, and maintenance staff, to gather insights and perspectives.

Expected Outcomes

As a class, brainstorm on the outcomes that should come from the assessment?



Expected Outcomes

The expected outcomes of this assessment include:

- A comprehensive report outlining U101's strengths and weaknesses compared to WindPower standards.
- Detailed recommendations for improving U101's cybersecurity efficiency, cost effectiveness, and reliability.
- Actionable insights to guide U101's decision-making and implementation of operational improvements.

Post Site Visit - General Observations

• Documentation

- The current asset inventory is incomplete and missing important information.
- Proper architecture and network diagrams are not available to reveal logical and physical network connections between assets.
- Interconnection between U101–U103 is not available.

• Antivirus

- Most of endpoints have antivirus software.
- There is no central management for antivirus software.
- Stand-alone systems do not have antivirus software, but they have manual scanning procedures.

Post Site Visit - General Observations

• Backups

- Network connected computer-based systems are automatically backed up using Windows Server Backup (WSB).
- For PLCs, there is a manual backup procedure.
- Most HMI panels do not have backup capabilities.

• DCS and Safety systems

- The DCS network is not segregated from the safety network on each location.
- Same username and password is being used by all operators for using workstation
- Only one engineer know the process of resetting password if lost or expired.

Post Site Visit - General Observations

• Operating System Configuration

- All Windows OS systems were hardened by the respective vendor guidelines, but there are no controls in place to verify if this is still the case.
- There is not hardening procedure, each vendor has done their own way.
- Logs are not enabled for applications and security.

• Network Management

- Process engineer was using telnet to access network switches in Level 2.
- Network connecting PLC to HMI is single and routed using metal conduits and separate cable tray.
- Engineer sitting in U101 can take RDP of workstation of U105 without any approval from U105, was editing log rotation of machine.

Assessment Output

As a class, write up their the observations in an assessment report template based on the FRs.

FR	Requirement	Recommendation	Results	Score

Total

Score (Total/100X) %



15

X = No. of rows

Assessment Output

SR	Requirement	Recommendation	Results	Score
FR1	Identification and Authentication	All human users shall be uniquely identified and authenticated.	Operators are sharing same user name and passwords	40
FR2	Use Control	The control system should be set up to produce auditable events into the system log.	Logs are not enabled on the windows for application and security	20
FR3	System Integrity	Communication integrity: Transmitted information should be protected.	Telnet is in use, so not compliant to communication integrity	45
FR4	Data Confidentiality	Information like passwords should be secured and protected.	Passwords are shared and telnet also show password in plaintext	60
FR5	Restricted Data Flow	Zone boundary protection should be enforced at zone boundaries.	Remote access is not configured or boundary protection is not implemented	25
FR6	Timely response to events	The audit logs should (only) be accessible for authorised users from a read-only device.	Engineer was able to change log rotation from other unit.	67
FR7	Resource Availability	The IACS should be set up so that up-to-date backups are available for full system recovery.	Some backups are not taken, so can be tough when full system recovery is required.	56

Total 313
Score (Total/700) 44.7%

Learning objectives

- Understand the importance of securing IACS and the unique challenges they face compared to IT systems. ✓
- Gain a thorough understanding of the Purdue model, a widely recognised framework for classifying and securing IACS environments. ✓
- Appreciate the key principles and structure of the ISA/IEC 62443 standard, a comprehensive framework for industrial cybersecurity. ✓
- Identify and apply the foundational requirements, terminology, and concepts outlined in the ISA/IEC 62443 Part 1: General standard. ✓



Thank you

engcore
advancing technology