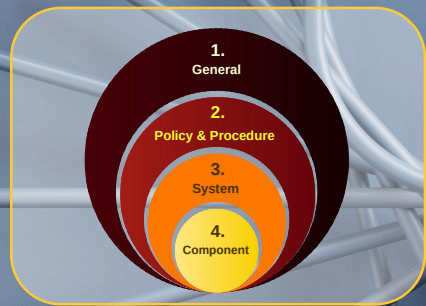


## Topic 3.2 ISA/IEC 62443

Dr Diarmuid Ó Briain

14 Feb 2024



## 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>

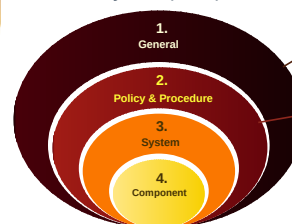
## Learning objectives

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

- define the elements of a comprehensive IACS CSMS.
- explain the concept of maturity levels and how to assess and improve the cybersecurity maturity of an IACS organisation.
- understand the requirements for security programme ratings, patch management, and security program requirements for service providers.
- gain insights into the guidance provided for IACS asset owners to help them implement and maintain a secure IACS environment.
- describe the security technologies and requirements for IACS systems, and the secure product development lifecycle for IACS components.

## ISA/IEC 62443 Part 2: Policy and Procedure

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: IACS security lifecycle and use cases

#### Part 2-1: Establishing an IACS Security programme

- Part 2-2: IACS 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 IACS asset owners

## Part 2-1: Establishing an IACS Security Programme

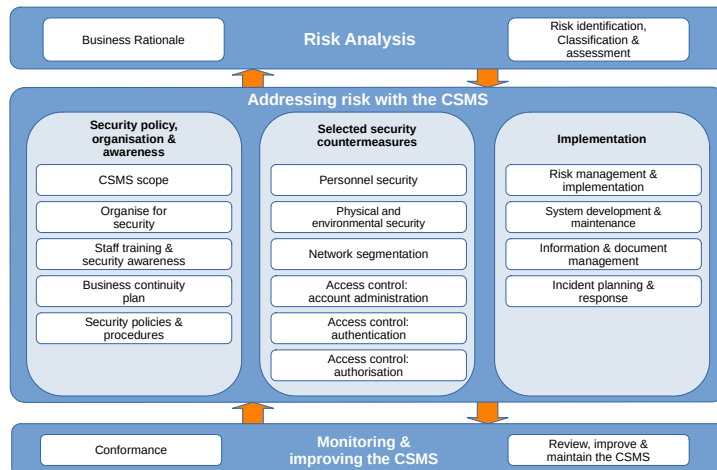
- The standard applies to all organisations that own, operate, or maintain IACS.
- The standard also applies to all types of IACS, including:
  - Process Control Systems (PCS)
  - Supervisory Control and Data Acquisition (SCADA) systems
  - Distributed Control Systems (DCS)
  - Manufacturing Execution Systems (MES)
  - Industrial Automation Systems (IAS)

## Part 2-1: Establishing an IACS Security Programme

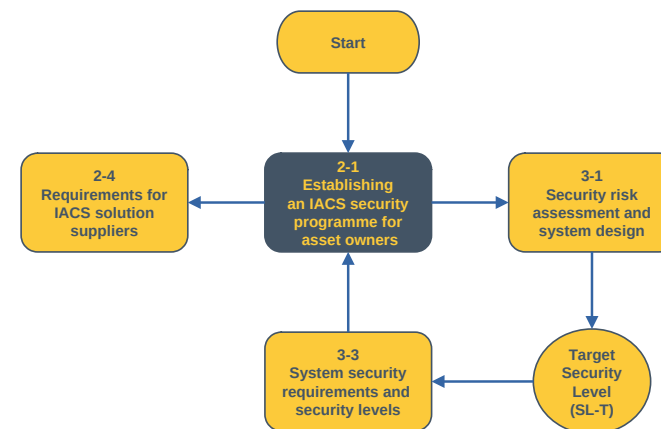
### • Key Requirements

- Policy and organisation
- Resource management
- Process management
- Communication and cooperation

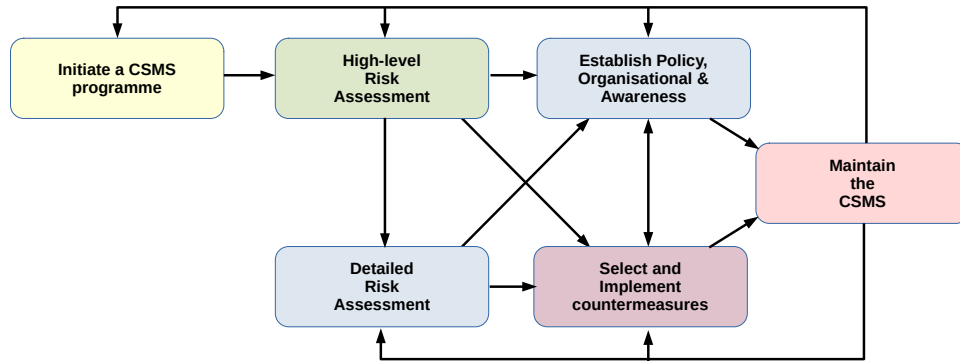
## Part 2-1: Categories of a CSMS



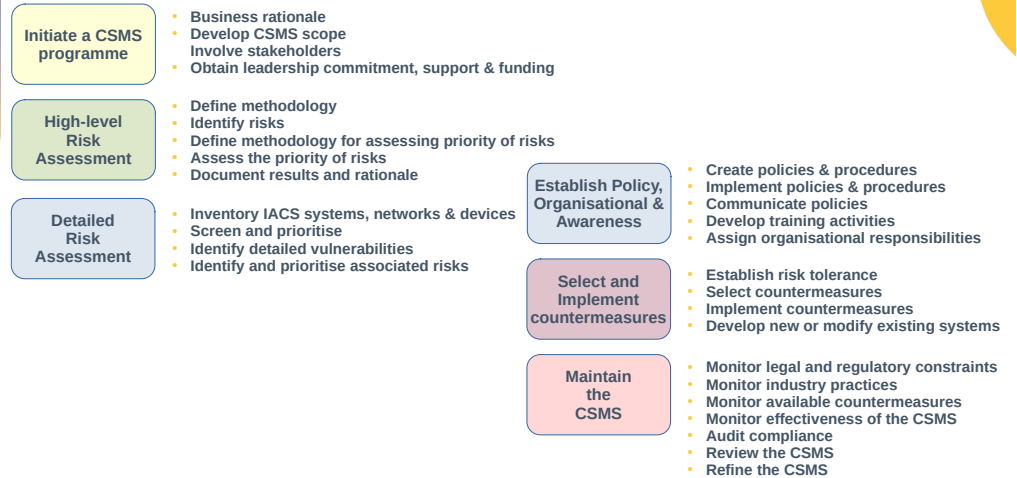
## ISA/IEC 62443 relationship between parts



## Process to develop a CSMS



## Process to develop a CSMS



## Part 2-2: ICAS Security programme ratings

- Set of levels of security, from Category 0 (lowest) to Category 4 (highest).
- These requirements cover a wide range of areas, including:
  - Asset management
  - Communication security
  - Application security
  - Operational security
  - Maintenance security

## Part 2-3: Patch Management

- Set of requirements for patch management, including:
  - Identifying and classifying vulnerabilities
  - Prioritising vulnerabilities
  - Deploying patches
  - Testing patches
  - Monitoring patch deployment
  - Remediating non-deployed patches

## Part 2-4: Security programme requirements for IACS service providers

- Part 2-4 applies to all organisations that provide IACS services such as:
  - Design and development of IACS
  - Manufacturing of IACS
  - Installation and commissioning of IACS
  - Maintenance and support of IACS
  - Operation and monitoring of IACS
  - Outsourcing of IACS services

## Part 2-4: Security programme requirements for IACS service providers

- The standard also applies to organisations that provide services that are not directly related to IACS, but that could impact the security of IACS such as:
  - Networking and telecommunications
  - Security consulting
  - Vulnerability management
  - Security training and awareness

## Part 2-4: Security programme requirements for IACS service providers

Feature	ISA/IEC 62443-2-1	ISA/IEC 62443-2-4
Target audience	IACS owners and operators	IACS service providers
Focus	Establish and implement a CSMS	Establish and implement a cybersecurity programme for service providers
Scope	Policy and organisation, resource management, process management, and communication and cooperation	Policy and organisation, resource management, process management, and communication and cooperation

## Part 2-4

- The security programmes implementing these requirements are **expected to be independent of different releases** of the products used in the automation solution.
- The requirements are defined in terms of the **capabilities that these security programmes** are required to provide.
- The standard recognises that security programmes evolve and that capabilities go through a life cycle of their own, often starting as completely manual and evolving over time to become more formal, more consistent, and more effective 62443-2-4 addresses this issue of evolving capabilities by **defining a maturity model to be used with** the application of this standard.
- **Service providers and asset owners should negotiate** and agree on which of these required capabilities are to be provided and how.
- **Encourage service providers** to implement the required capabilities so they can be adaptable to a wide variety of asset owners.
- The **maturity model** also allows asset owners to understand the maturity of a specific service provider's capabilities better

## Part 2-4

- Part 2-4 is relevant for asset owners and addresses capabilities of service providers that may support or undermine the security maturity of asset owners.
- Contains security requirements for providers of integration and maintenance services for IACS.
- The standard specifies requirements for **security capabilities for IACS service providers** that they can offer to the asset owner during integration and maintenance activities of an automation solution.
- It is related to Part 2-1, which describes requirements for the security management system of the asset owner.
- Part 2-4 can be used by asset owners to request specific security capabilities from the service provider.
- Part 2-4 can be used by asset owners to determine whether or not a specific service provider's security program includes the capabilities that the asset owner needs.

## Part 2-5: Guidance for ICAS asset owners

- Provides implementation guidance for ICAS asset owners on how they can improve the security of their assets.
- The standard provides guidance on a wide range of topics, including:
  - Asset identification
  - Asset classification
  - Asset protection
  - Asset management
  - Asset disposal

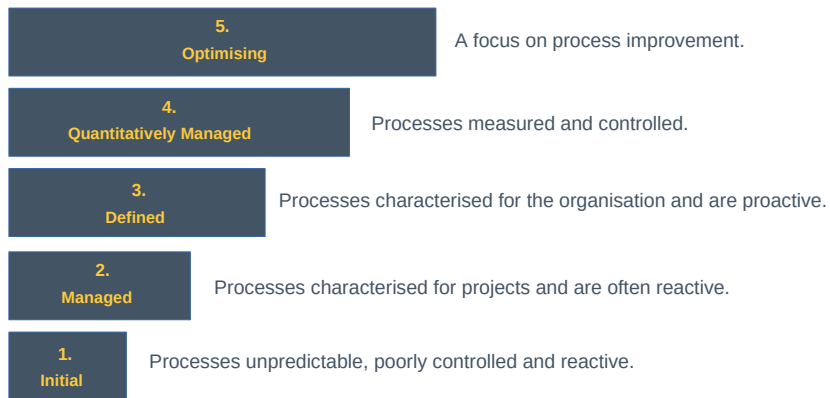
## Part 2-5: Guidance for ICAS asset owners

- The standard also provides guidance on how to implement the necessary security controls to protect IACS assets. These controls include:
  - Physical security
  - Environmental security
  - Data security
  - Network security
  - Application security
  - Operational security
  - Maintenance security

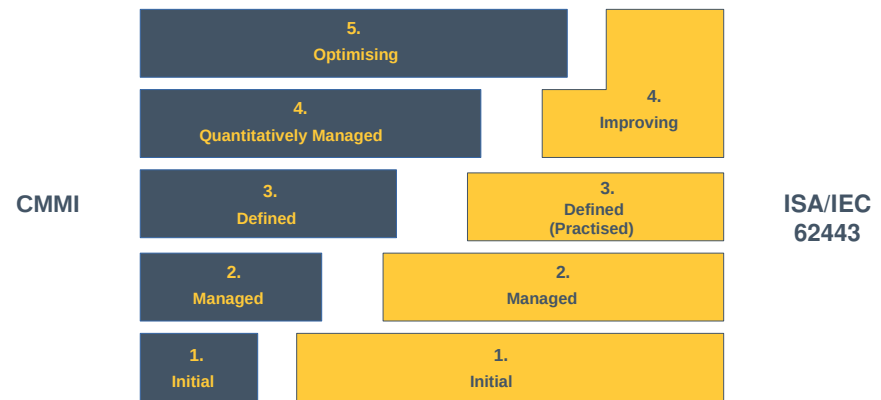
## Part 2-5: Guidance for ICAS asset owners

- Additionally, the standard provides guidance on how to assess the effectiveness of the security controls, including:
  - Vulnerability assessments
  - Penetration testing
  - Incident response

## CMMI

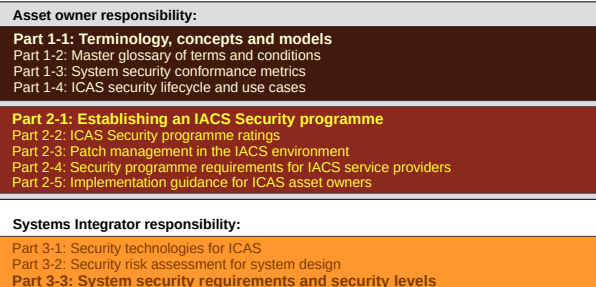
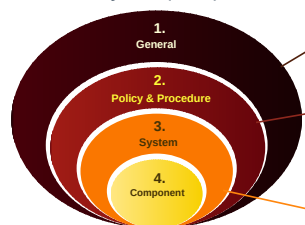


## ICAS Maturity compared to CMMI



## ISA/IEC 62443 Part 3

### Industrial Automation and Control System (IACS)



## Part 3-1 - Implement security technologies for IACS

- Technical specification that defines the requirements for securing IACS by providing guidance on how to implement security technologies for IACS.
- This is important because IACS are increasingly being targeted by cyberattacks.
- Assists organisations to significantly reduce their risk of cyberattacks and protect their IACS from harm.

## Part 3-1 - Implement security technologies for IACS

- **Key Requirements**
  - Network Segmentation
  - Access Control
  - Encryption
  - IDS/IPS
  - Honeypots
  - SIEM

## Part 3-1 - Implement security technologies for IACS

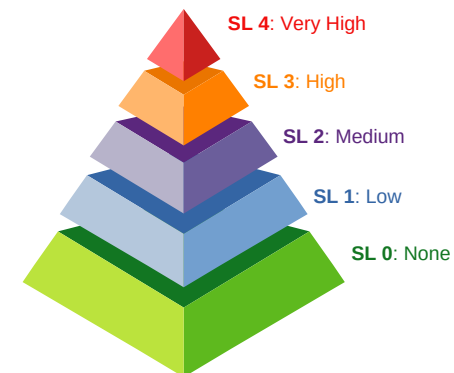
- **Security Requirements**
  - Availability
  - Integrity
  - Confidentiality
  - Accessibility

## Part 3-2 - Security risk assessment for system design

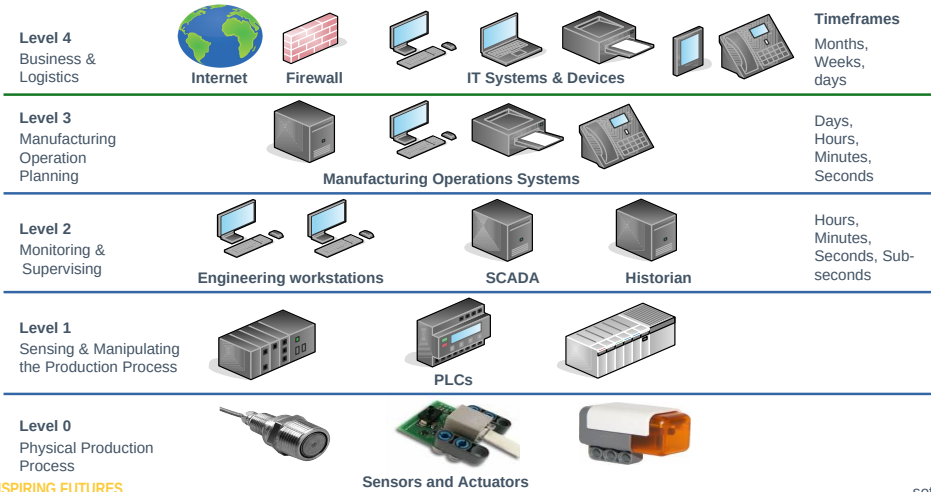
- defines the requirements for conducting security risk assessments for IACS:
  - Identify assets
  - Analyse threats
  - Evaluate vulnerabilities
  - Assess risk
- Also defines a set of security requirements for each step of the security risk assessment process.

## Part 3-3 - System security requirements and security levels

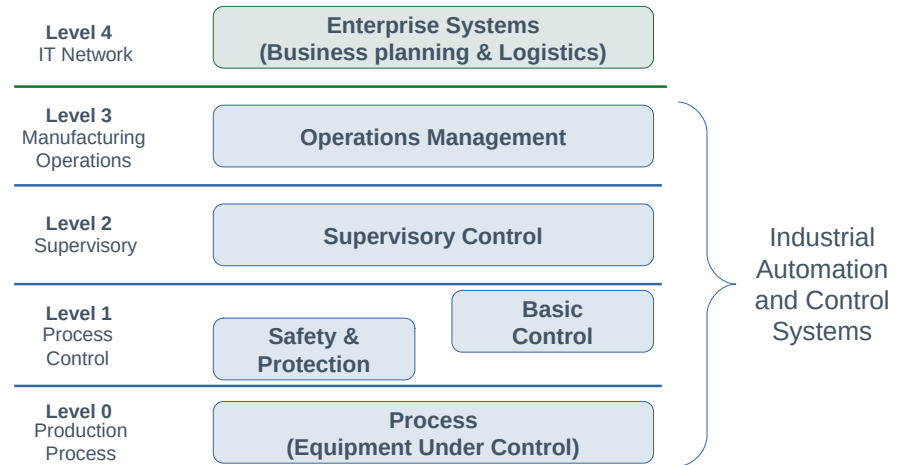
- defines a 4-level security classification scheme for IACS:



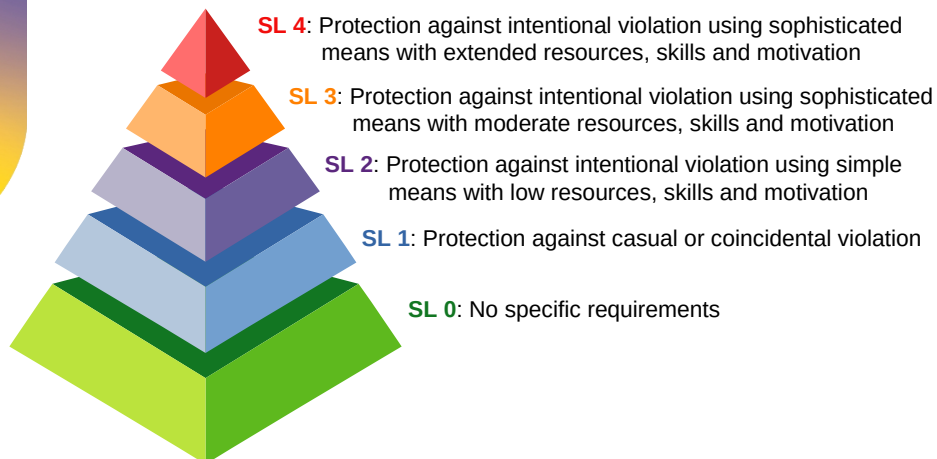
## ISA-95 Reference Model



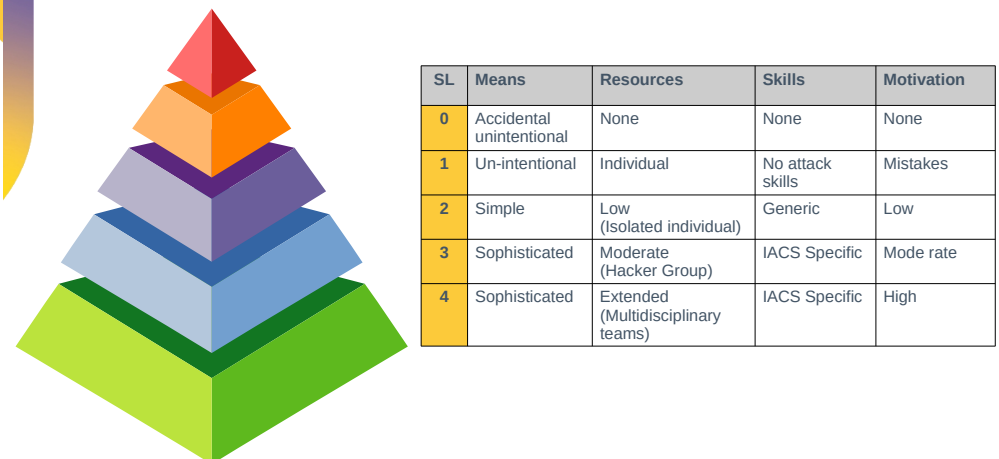
## ISA-99 Reference Model



## Security Levels



## Security Levels



SL	Means	Resources	Skills	Motivation
0	Accidental unintentional	None	None	None
1	Un-intentional	Individual	No attack skills	Mistakes
2	Simple	Low (Isolated individual)	Generic	Low
3	Sophisticated	Moderate (Hacker Group)	IACS Specific	Mode rate
4	Sophisticated	Extended (Multidisciplinary teams)	IACS Specific	High



## Security Level Controls

The following controls are mandated for SL4:

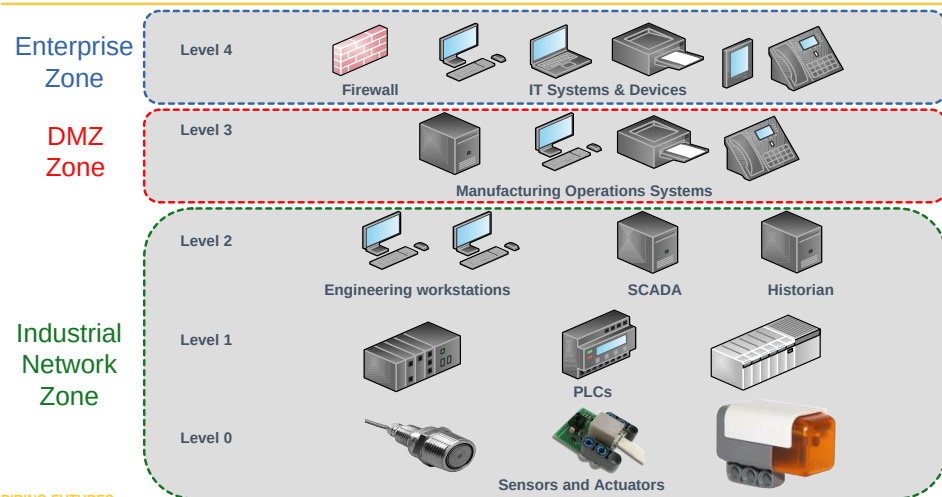
- Access Control Mechanisms
- Auditing and Logging
- Date Integrity Protection
- Configuration Management
- Identity and Access Management
- Vulnerability Management
- Security Awareness Training
- Segmentation
- Security Testing
- Incident Response

## Security Level Types

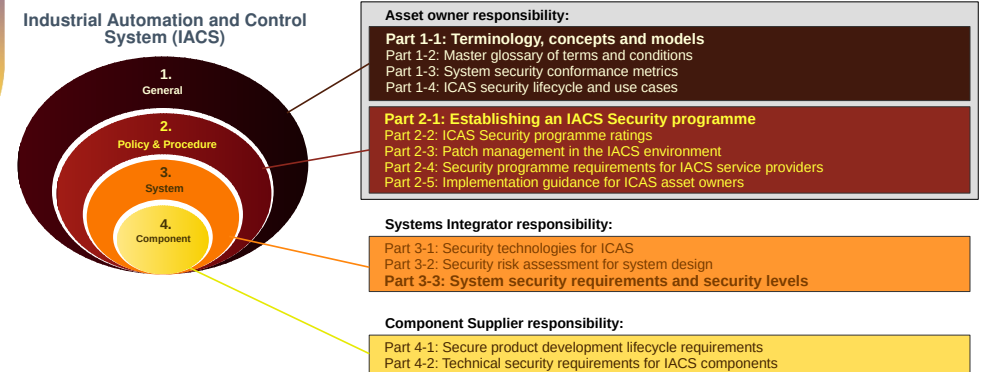
SLs are grouped into three types:

- **Target SLs (SL-T):**
  - These are the desired level of security for an automation solution.
  - A System or Component can achieve SL-T natively without additional countermeasures.
- **Achieved SLs (SL-A):**
  - These are the actual level of security for an IACS.
  - The SL-A are determined as a result of Risk Assessment.
  - They are used to select products and design additional countermeasures during the integration phase of the IACS lifecycle.
- **Capability SLs (SL-C):**
  - These are the security levels that components or systems can provide when properly configured.

## Zones and Conduits



## ISA/IEC 62443 Part 4



## Part 4-1 - Secure product development lifecycle

- Technical specification that defines the requirements the requirements for implementing a secure product development lifecycle for IACS.
- The specification describes the requirements for the Security Development Lifecycle (SDL) of OT System and Component products.

## Part 4-1 - Secure product development lifecycle

### • Key Requirement Categories

- Planning
- Design
- Development
- Testing
- Deployment
- Operation
- Decommissioning

## Part 4-2 – Security Requirements for Components

- Provide guidance on how to select, install, and maintain secure IACS components through the definition of Common Cyber Security Constraints (CCSC).
- This is important because IACS components are often the weakest link in an IACS security posture.

## Part 4-2 – Security Requirements for Components

### • Key Requirement Categories

- Identification and classification
- Security policy
- Vulnerability management
- Protection against unauthorised access
- Security updates
- The standard also defines a set of security constraints.

## Part 4-2 – Security Requirements for Components

### • Threat Modelling

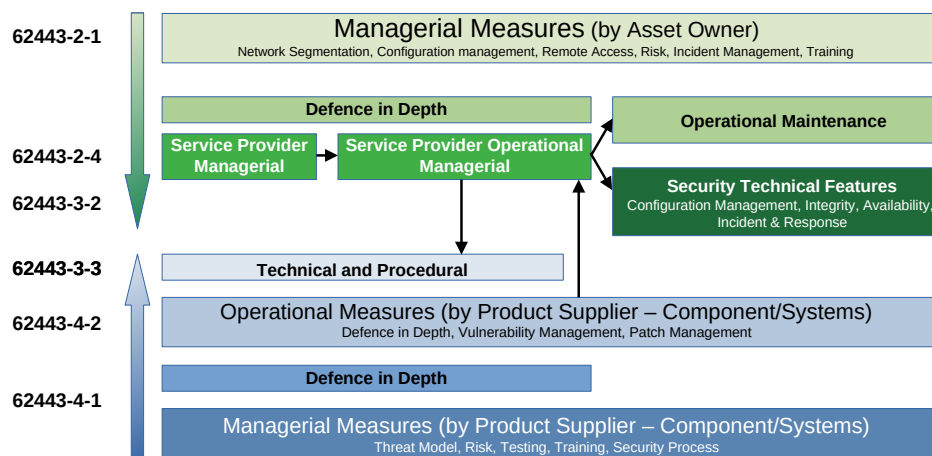
- Systematic process to identify data flows, trust boundaries, attack vectors, and potential threats to the ICAS.
- The vendor must address any security issues that are identified in the threat modelling process before product release.
- The threat modelling process must be updated between releases and changes addressed before each release.

## Part 4-2 – Security Requirements for Components

### • Common Cyber Security Constraints

- **CCSC 1:** describes that components must take into account the general security characteristics of the system in which they are used.
- **CCSC 2:** specifies that the technical requirements that the component cannot meet itself can be met by compensating countermeasures at system level.
- **CCSC 3:** requires that the Principal of Least Privilege (PoLP) is applied in the component.
- **CCSC 4:** requires that the component is developed and supported by a Part 4-1 compliant development processes.

## Dependencies



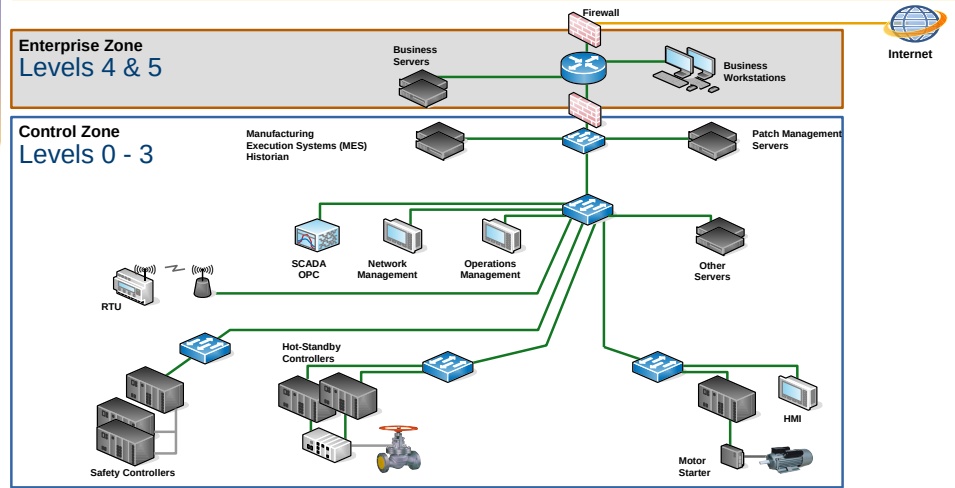
## Summary

### • ISA/IEC 62443 series of standards

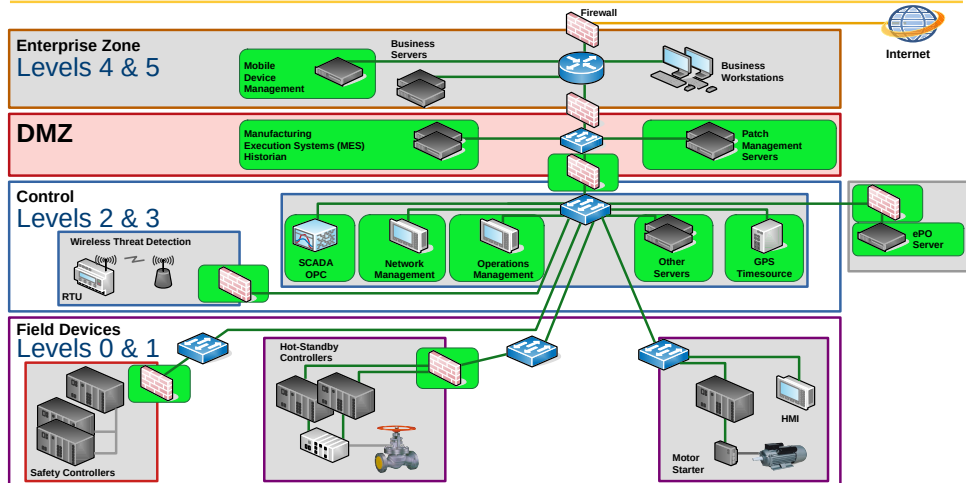
- **Security for product development lifecycle:** provides guidance on how to secure IACS products throughout the product development lifecycle, from requirements gathering to deployment and decommissioning.
- **Security risk assessment:** provides guidance on how to identify, assess, and prioritise security risks in IACS environments.
- **Security levels:** defines a four-level security classification system for IACS assets.
- **Security for components:** provides guidance on how to secure IACS components, such as PLCs and HMIs.
- **Security of communication networks:** provides guidance on how to secure IACS communication networks, such as SCADA networks.

# Example

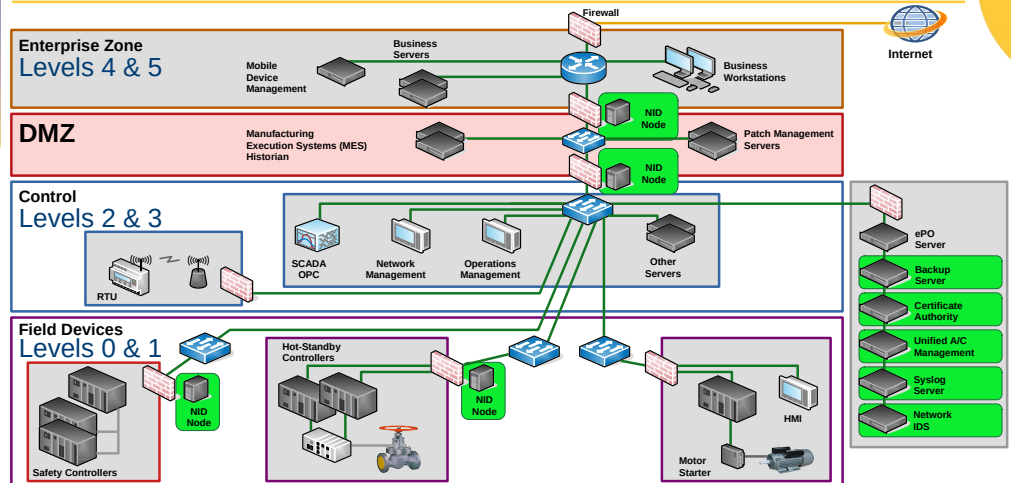
## Sample Network



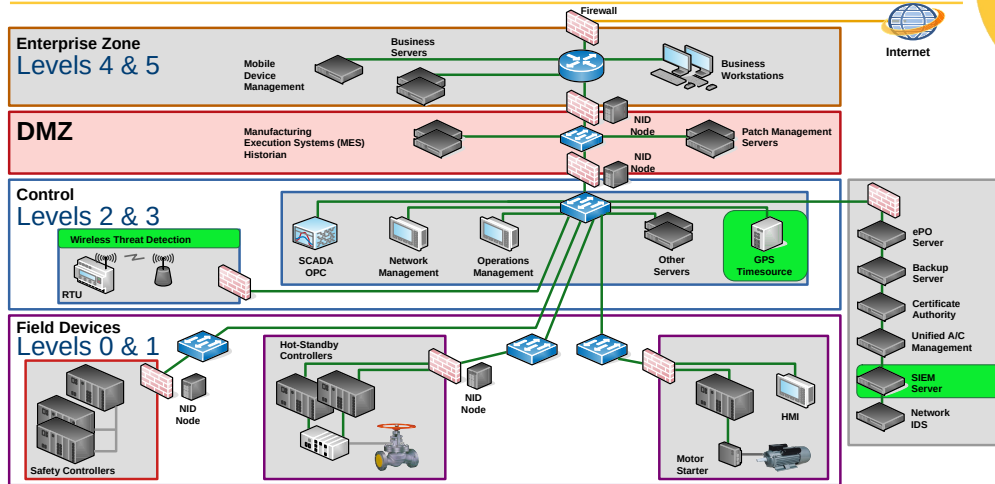
## Security Level 1



## Security Level 2



## Application of Security Level 3 controls



**Revision**

**QUIZ**

SE TU  
Ollscoil  
Teicneolaíochta  
an Oirdeiscirt  
South East  
Technological  
University

INSPIRING FUTURES

setu.ie | 50

## Question 1

- Select the incorrect statement from the following:
  - SL-0: No specific requirements or security protection are necessary
  - SL-1: Protection against casual or coincidental violation
  - SL-3: Protection against intentional violation using simple means with low resources, generic skills, and low motivation
  - SL-4: Protection against intentional violation using sophisticated means with extended resources, IACS-specific skills and high motivation



## Question 1

- Select the incorrect statement from the following:
  - SL-0: No specific requirements or security protection are necessary
  - SL-1: Protection against casual or coincidental violation
  - SL-3: Protection against intentional violation using simple means with low resources, generic skills, and low motivation
  - SL-4: Protection against intentional violation using sophisticated means with extended resources, IACS-specific skills and high motivation



## Question 2

- Which type of security level defines what a component or system is capable of meeting?:
  - Capability security level
  - Achieved security level
  - Design security level
  - Target security level



## Question 2

- Which type of security level defines what a component or system is capable of meeting?:
  - Capability security level
  - Achieved security level
  - Design security level
  - Target security level



## Question 3

- Which of the ISA/IEC 62443 standards focuses on the processes of developing securing products?:
  - ISA/IEC 62443-1-1
  - ISA/IEC 62443-3-2
  - ISA/IEC 62443-3-3
  - ISA/IEC 62443-4-1



## Question 3

- Which of the ISA/IEC 62443 standards focuses on the processes of developing securing products?:
  - ISA/IEC 62443-1-1
  - ISA/IEC 62443-3-2
  - ISA/IEC 62443-3-3
  - ISA/IEC 62443-4-1



## Question 4

- Which of the following ISA-99 Reference model is named correctly?:

- Level 1 – Supervisory Control
- Level 2 – Quality Control
- Level 1 – Manufacturing Operations
- Level 1 – Process



setu.ie | 57

## Question 4

- Which of the following ISA-99 Reference model is named correctly?:

- Level 1 – Supervisory Control
- Level 2 – Quality Control
- Level 3 – Manufacturing Operations
- Level 4 – Process



setu.ie | 58

## Question 5

- Which of the ISA 62443 standards focuses on patch management?:

- ISA/IEC 62443-1-3
- ISA/IEC 62443-2-3
- ISA/IEC 62443-3-1
- ISA/IEC 62443-4-1



setu.ie | 59

## Question 5

- Which of the ISA 62443 standards focuses on patch management?:

- ISA/IEC 62443-1-3
- ISA/IEC 62443-2-3
- ISA/IEC 62443-3-1
- ISA/IEC 62443-4-1



setu.ie | 60

## Learning objectives

- Define the elements of a comprehensive IACS CSMS. ✓
- Explain the concept of maturity levels and how to assess and improve the cybersecurity maturity of an IACS organisation. ✓
- Understand the requirements for security programme ratings, patch management, and security program requirements for service providers. ✓
- Gain insights into the guidance provided for IACS asset owners to help them implement and maintain a secure IACS environment. ✓
- Describe the security technologies and requirements for IACS systems, and the secure product development lifecycle for IACS components. ✓



**TUS**  
Oibiceil Teicneolaíochta na Sionainne  
Lár Tíre, An Bhaile na Lár  
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



Thank you

