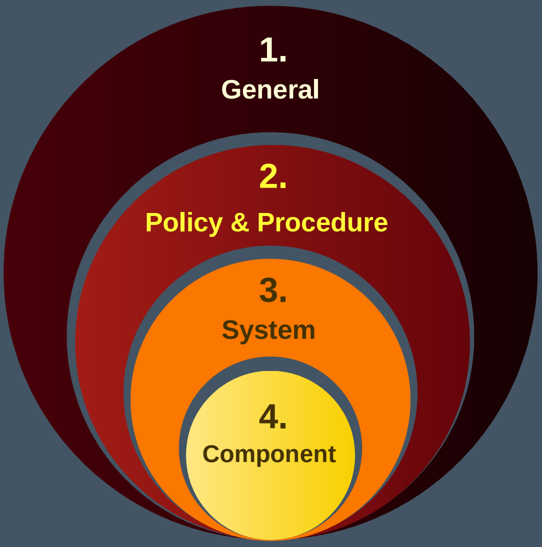
Cybersecurity for Industrial Networks

Topic 3.2
ISA/IEC 62443



Dr Diarmuid Ó Briain

Version: 1.0

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Dr Diarmuid Ó Briain

Table of Contents

Illustration Index

1 Introduction

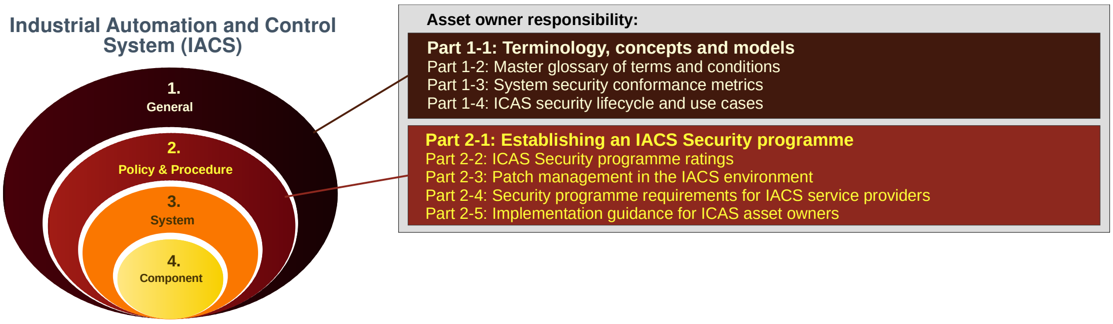
Topic 3.1 provided an overview of the ISA/IEC 62443 standard, a comprehensive framework for industrial cybersecurity. This chapter dives into Parts 2, 3 and 4 of the standard, which focuses on the policies and procedures required to implement and maintain a secure IACS environment, systems and components.

1.1 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 security management system (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.

2 ISA/IEC 62443 Part 2: Policy and Procedure



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: Establishing an IACS Security programme
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

Figure 1: ISA/IEC 62443 Part 2: Policy and Procedure

The International Society of Automation (ISA)/International Electrotechnical Commission (IEC) (ISA/IEC) 62443 [1] Part 2: is a set of standards that define policies and procedures related to the establishment and maintenance of an Industrial Automation and Control Systems (IACS) security programme. They may be implemented by asset owners and service providers; however, these standards remain the responsibility of the asset owner.

2.1 ISA/IEC 62443-2-1: Establishing an IACS Security Programme

Part 2-1: Establishing an IACS Security Programme is a technical specification that defines the requirements for establishing and implementing an effective IACS Cyber Security Management System (CSMS).

2.1.1 Scope

The standard applies to all organisations that own, operate, or maintain IACS. This includes organisations of all sizes, from Small and Medium-sized Enterprises (SME) to large multinational corporations. 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).

2.1.2 Key requirements

The standard contains a number of key requirements for establishing and implementing an effective IACS CSMS. These requirements are divided into four main categories:

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

The specific requirements within each category are detailed in the standard. However, some of the key requirements include:

- **Establishing a cybersecurity policy**: This policy should define the organisation's commitment to IACS cybersecurity and outline the roles and responsibilities of different stakeholders.
- **Assigning cybersecurity roles and responsibilities**: Clearly define the roles and responsibilities of different individuals and teams within the organisation for IACS cybersecurity.
- **Developing and implementing cybersecurity procedures**: Create and implement procedures for managing IACS security risks, conducting security assessments, responding to security incidents, and maintaining security documentation.
- **Training employees on cybersecurity**: Provide regular training to employees on IACS cybersecurity risks, threats, and controls.
- **Communicating cybersecurity risks and incidents**: Communicate cybersecurity risks and incidents to employees, stakeholders, and regulators.

2.2 Elements of a CSMS

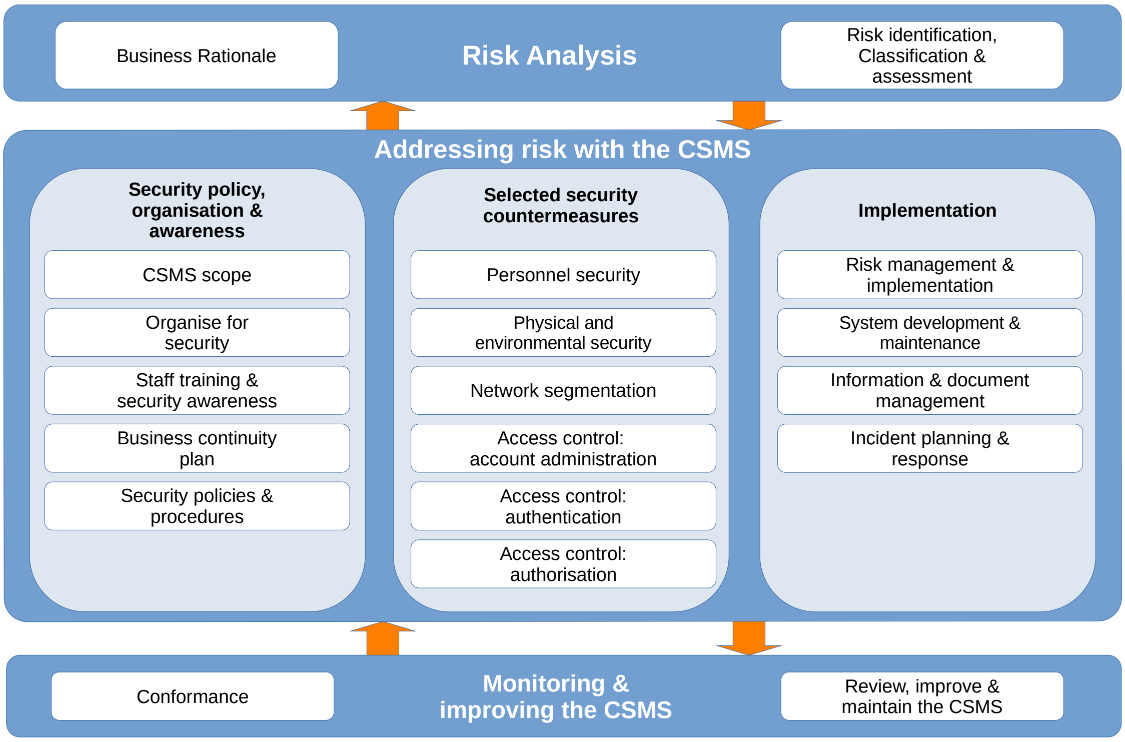

Business Rationale
Risk Analysis
Risk identification, Classification & assessment
Addressing risk with the CSMS
Security policy, organisation & awareness
CSMS scope
Organise for security
Staff training & security awareness
Business continuity plan
Security policies & procedures
Selected security countermeasures
Personnel security
Physical and environmental security
Network segmentation
Access control: account administration
Access control: authentication
Access control: authorisation
Implementation
Risk management & implementation
System development & maintenance
Information & document management
Incident planning & response
Conformance
Monitoring & improving the CSMS
Review, improve & maintain the CSMS

Figure 2: Categories of a CSMS

The diagram in Figure 2 illustrates the elements that constitute a CSMS for IACS in order to protect IACS against cyber attacks.

The elements are presented in three main categories:

- Risk analysis
- Addressing risk with the CSMS
- Monitoring and improving the CSMS

Each category is further sub-divided into element groups and/or elements and the relationship between the categories, element groups and elements can be seen in the figure. Each element lists the objective of the element, a basic description of the element, a rationale to explain why the element is included, and the requirements for that element.

Risk Analysis

- **Business rationale:** is based on the nature and magnitude of financial, health, safety, environmental, and other potential consequences should IACS cyber incidents occur. Since the purpose of investing in cyber security is to lower risk, it is driven by an understanding of level of risk and potential mitigations.
- **Risk identification, Classification & assessment**: is the first step in the process of addressing risk with the CSMS. It involves identifying potential threats to the organisation, classifying them by severity and likelihood, and assessing the impact they could have on the business.

Addressing Risk with the CSMS

- **Security policies, organisation and awareness**: The first element group in this category discusses the development of the basic cyber security policies, the entities responsible for cyber security, and the awareness within the organisation of cyber security issues.
- **Selected security countermeasures**: The elements within this group discuss some of the main types of security controls that are part of a well-designed CSMS. This document does not attempt to describe the full implementation of any of these selected security countermeasures. It discusses many of the policy, procedure, and practice issues related to these particular security countermeasures.
- **Implementation**: This element within this group discusses issues related to implementing the CSMS.

Monitoring & improving the CSMS

Involves both ensuring that the CSMS is being used, and reviewing the CSMS itself for effectiveness.

- **Conformance** with a CSMS means the organisation is adhering to its stated policies, executing the procedures at the correct time, and producing the appropriate reports to allow for future review.
- **Review, improve & maintain the CSMS**: Review and monitoring are required for the CSMS to remain effective, since the CSMS must respond to changes in internal and external threats, vulnerabilities, and consequences, as well as changes in risk tolerance, legal requirements, and evolving technical and non-technical approaches to risk mitigation.

2.2.1 Process to develop a CSMS

The diagram in Figure 3 illustrates the requirements for IACS security management systems. The diagram shows the four main phases of IACS security management:

- **Establishing an IACS security programme (2-1)**: This phase involves identifying, classifying, and managing IACS assets. It also includes developing security requirements for IACS solutions.
- **Planning and Organisation (2-4)**: This phase involves defining the scope of the security management system, establishing roles and responsibilities, and developing policies and procedures.
- **Security Risk Management (3-1)**: This phase involves identifying, analysing, and evaluating security risks to IACS. It also includes developing security controls to mitigate those risks.
- **Security Operation (3-3)**: This phase involves implementing, monitoring, and maintaining security controls. It also includes performing security audits and incident response.

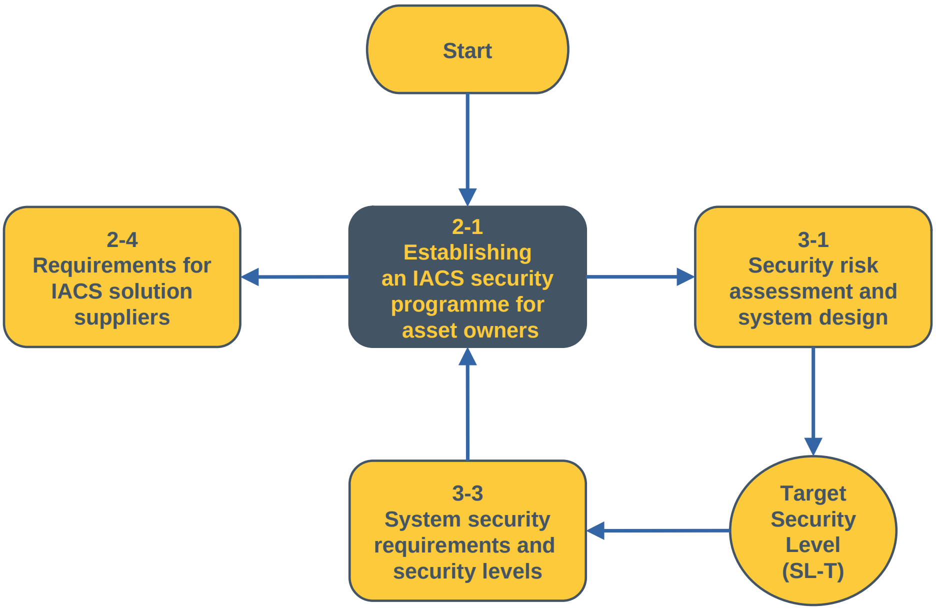


Figure 3: Broad Relationship between ISA/IEC 62443 Standards

The diagram also illustrates that the requirements for each phase are linked to the requirements for the Security Level – Target (SL-T). SL-T is a measure of the overall security of an IACS system. It is determined by the organisation's risk tolerance and the criticality of the IACS system.

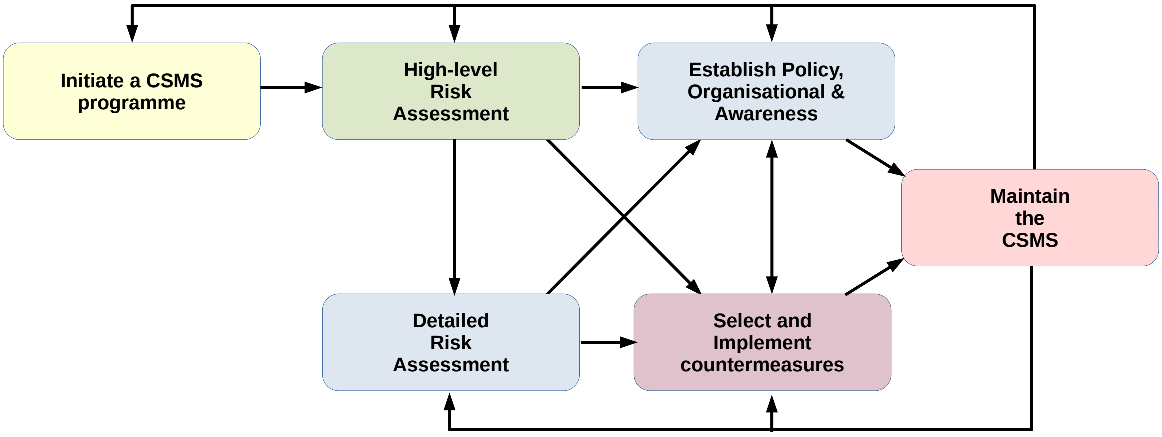


Figure 4: Process to develop a CSMS

Figure 4 outlines the process of establishing the CSMS for IACS. Here's a breakdown of the key components:

- **Initiating the CSMS programme**: This involves establishing the scope, objectives, and resources for the CSMS programme.
- **High-level risk assessment**: This identifies and prioritises the security risks to the IACS based on a high-level understanding of the system and its assets.
- **Detailed risk assessment**: This conducts a more in-depth analysis of the identified risks, considering vulnerabilities, threats, and potential consequences.
- **Establish policy, organisation, and awareness**: This involves developing security policies, procedures, and training programmes to address the identified risks.
- **Select and implement countermeasures**: This involves choosing and implementing security controls to mitigate the identified risks.
- **Maintain the CSMS**: This involves continuously monitoring, reviewing, and updating the CSMS to ensure its effectiveness.

While the diagram emphasises the importance of risk assessment as the foundation for all subsequent steps, it also highlights the need for a coordinated approach involving technical and non-technical aspects of cybersecurity as well as acknowledging the balance between security and cost, where optimal security needs to be achieved within budgetary constraints.

2.3 ISA/IEC 62443-2-2: IACS Security programme ratings

The Part 2-2 technical specification defines the requirements for assessing and improving the security of IACS. The standard offers a methodology for assessing the level of cybersecurity protection provided by an operational IACS.

It does this by defining a set of levels of security, from Category 0 (lowest security) to Category 4 (highest security). Organisations can use these levels to assess their current security posture and set goals for improvement. These requirements cover a wide range of areas, including:

- **Asset management**: Identifying, classifying, and protecting IACS assets
- **Communication security**: Securing IACS networks and communications
- **Application security**: Securing IACS applications and databases
- **Operational security**: Securing IACS operations and procedures
- **Maintenance security**: Securing IACS maintenance and updates.

2.4 ISA/IEC 62443-2-3: Patch Management

The Part 2-3 technical specification defines the requirements for managing security patches for IACS. Patch management is a critical part of any IACS security programme as it helps to ensure that IACS are up to date with the latest security patches, which can help to protect them from vulnerabilities that attackers can exploit.

The standard defines a set of requirements for patch management, including:

- **Identifying and classifying vulnerabilities**: Organisations need to identify and classify vulnerabilities in their IACS systems. This can be done by using vulnerability scanning tools and by keeping up with security advisories.
- **Prioritising vulnerabilities**: Once vulnerabilities have been identified, they need to be prioritised. This means that organisations need to determine which vulnerabilities are most critical to fix.
- **Deploying patches**: Once vulnerabilities have been prioritised, patches need to be deployed to IACS systems. This can be done manually or automatically.
- **Testing patches**: Before patches are deployed, they need to be tested to make sure that they do not cause any problems with IACS systems.
- **Monitoring patch deployment**: Once patches have been deployed, organisations need to monitor them to make sure that they are working correctly.
- **Remediating non-deployed patches**: Organisations need to have a process for remediating patches that are not deployed. This may involve re-testing the patches or deploying them manually.

The standard also defines a set of requirements for the documentation of patch management activities. This documentation should include information about the vulnerabilities that have been identified, the prioritisation of vulnerabilities, the deployment of patches, the testing of patches, and the monitoring of patch deployment.

2.5 ISA/IEC 62443-2-4: Security programme requirements for service providers

ISA/IEC 62443 part 2-4 is a technical specification that defines the requirements for establishing and implementing an effective cybersecurity programme for IACS service providers. The standard applies to all organisations that provide IACS services. This includes organisations that provide the following services:

- 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.

The standard also applies to organisations that provide services that are not directly related to IACS, but that could impact the security of IACS. This includes organisations that provide the following services:

- Networking and telecommunications
- Security consulting
- Vulnerability management
- Security training and awareness.

While the standard demands robust security programmes for automation solutions, it acknowledges the dynamic nature of these programmes. It avoids locking them to specific product versions by focusing on **required capabilities**. As security matures, evolving from manual processes to automated and effective solutions, the standard offers a **maturity model** (IEC 62443-2-4) to guide implementation. This allows for negotiation between service providers and asset owners, defining **which capabilities are needed and how they will be delivered**. Encouraging the development of adaptable capabilities, the standard empowers asset owners to better understand the **maturity level** offered by different service providers, ensuring a secure and adaptable automation landscape.

Specifically for asset owners, Part 2-4 of the standard plays a crucial role in evaluating and securing their automation solutions. This part contains security requirements for integration and maintenance service providers (IACS) and directly addresses capabilities that can support or undermine their own security maturity. It specifies the security capabilities IACS providers can offer during integration and maintenance activities, outlining a clear framework for negotiation and collaboration. Additionally, its connection to Part 2-1, which describes asset owner security management systems, fosters a holistic approach to cybersecurity. Ultimately, Part 2-4 empowers asset owners to:

- **Request specific security capabilities**: from service providers, ensuring alignment with their security needs.
- **Evaluate potential service providers**: based on whether their security programs incorporate the required capabilities.
- **Negotiate and agree on the implementation**: of these capabilities, securing their automation solutions effectively.

By leveraging Part 2-4, asset owners gain a powerful tool to ensure the security maturity of their automation systems, fostering a collaborative and secure environment with service providers.

The requirements of this standard are similar to Part 2-1, which is a more general standard that can be applied to all organisations that own and operate IACS. Part 2-4 is a more specific standard that is focused on the unique needs of IACS service providers. The table in Figure 5 compares both standards.

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

Figure 5: Comparison between ISA/IEC 62443 Parts 2-1 and 2-4

Here are some examples of how Part 2-1 and Part 2-4 can be used together:

- An IACS owner and operator can use Part 2-1 to establish a CSMS and then use Part 2-4 to implement specific cybersecurity controls for their service providers.
- An IACS service provider can use Part 2-4 to implement cybersecurity controls that meet the requirements of their customers.

2.6 ISA/IEC 62443-2-5: Guidance for IACS asset owners

Part 2-5 provides implementation guidance for IACS asset owners on how they can improve the security of their assets. This standard applies to all IACS asset owners, including organisations that own, operate, install, maintain, and decommission IACS.

2.6.1 Key requirements

The standard provides guidance on a wide range of topics, including:

- **Asset identification**: Identifying and classifying IACS assets.
- **Asset classification**: Classifying IACS assets based on their criticality.
- **Asset protection**: Protecting IACS assets from unauthorised access, modification, or destruction.
- **Asset management**: Managing the lifecycle of IACS assets.
- **Asset disposal**: Disposing of IACS assets securely.

The standard also provides guidance on how to implement the necessary security controls to protect IACS assets. These controls include:

- **Physical security**: Protecting IACS assets from physical harm.
- **Environmental security**: Protecting IACS assets from environmental hazards.
- **Data security**: Protecting IACS data from unauthorised access, modification, or destruction.
- **Network security**: Protecting IACS networks from unauthorised access, modification, or destruction.
- **Application security**: Protecting IACS applications from unauthorised access, modification, or destruction.
- **Operational security**: Protecting IACS operations from unauthorised access, modification, or destruction.
- **Maintenance security**: Protecting IACS maintenance from unauthorised access, modification, or destruction.

Additionally, the standard provides guidance on how to assess the effectiveness of the security controls that have been implemented, including:

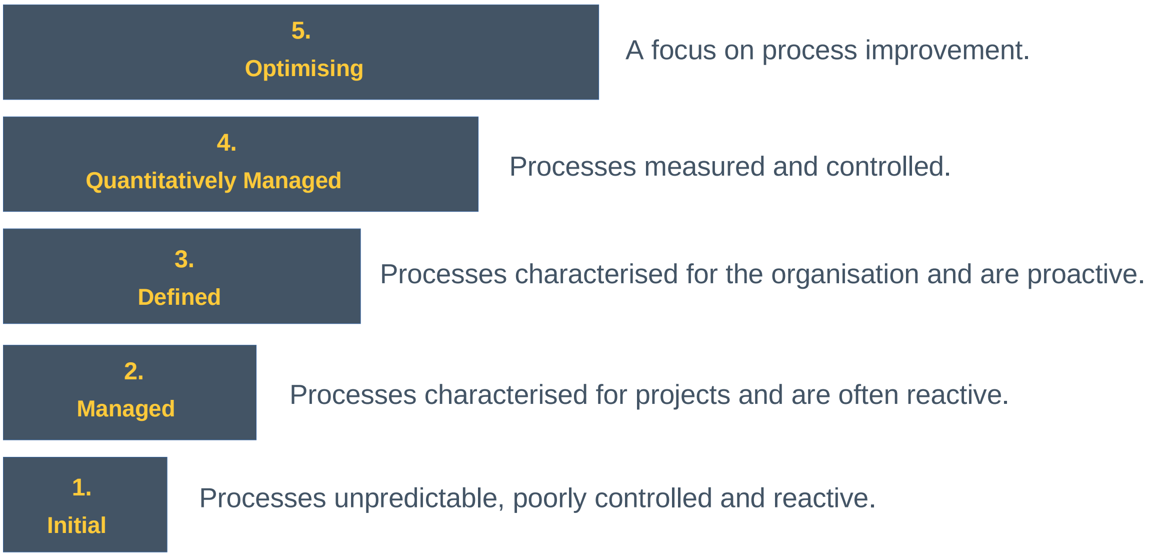
- **Vulnerability assessments**: Identifying and assessing vulnerabilities in IACS assets.
- **Penetration testing**: Testing the effectiveness of security controls against real-world attacks.
- **Incident response**: Preparing for, responding to, and recovering from cyberattacks.

2.7 Maturity Levels

The Capability Maturity Model Integration (CMMI) was developed at Carnegie Mellon University (CMU) and is administered by the CMMI Institute, a subsidiary of Information Systems Audit and Control Association (ISACA). It defines Maturity Levels for processes.

Maturity Levels (ML) refer to the resiliency, repeatability, measurability, and standardisation within a process. The CMMI for Development v1.3, define MLs as "*a defined evolutionary plateau for organisational process improvement. Each maturity level matures an important subset of the organisation's processes, preparing it to move to the next maturity level. The maturity levels are measured by the achievement of the specific and generic goals associated with each predefined set of process areas.*" (CMMI for Development v1.3, page 26).

While SLs are a measure of the strength of technical requirements, MLs are a measure of processes and how thoroughly requirements are met. They are a means of assessing organisational capabilities and represent an evolving concept in the standards whose purpose is to provide a benchmark for meeting requirements.



5. Optimising — A focus on process improvement.

4. Quantitatively Managed — Processes measured and controlled.

3. Defined — Processes characterised for the organisation and are proactive.

2. Managed — Processes characterised for projects and are often reactive.

1. Initial — Processes unpredictable, poorly controlled and reactive.

Figure 6: CMMI Maturity Levels

2.8 CMMI Maturity Levels

The CMMI is a process level improvement training and appraisal programme. The characteristics of the Maturity Levels are illustrated in Figure 6.

Maturity Level 1 - Initial

- Work efforts are ad-hoc.
- Tasks may be completed, but little or no process means that work may be delayed, inefficient, or extended beyond budgetary thresholds.

Maturity Level 2 – Managed

- Work efforts are repeatable, but performed in absence of a defined process.

Maturity Level 3 – Defined

- Work is completed via a standardised, documented process.

Maturity Level 4 – Quantitatively Managed

- Work is completed via a repeatable, measured, standardised process.
- Data and performance metrics are collected about the performance of the task.

Maturity Level 5 – Optimising

- Work is completed according to a virtuous cycle of continuous improvement.
- The data collected is used to guide improvements on how tasks are performed and can be optimised.

2.9 ISA/IEC 62443 Maturity Levels and CMMI

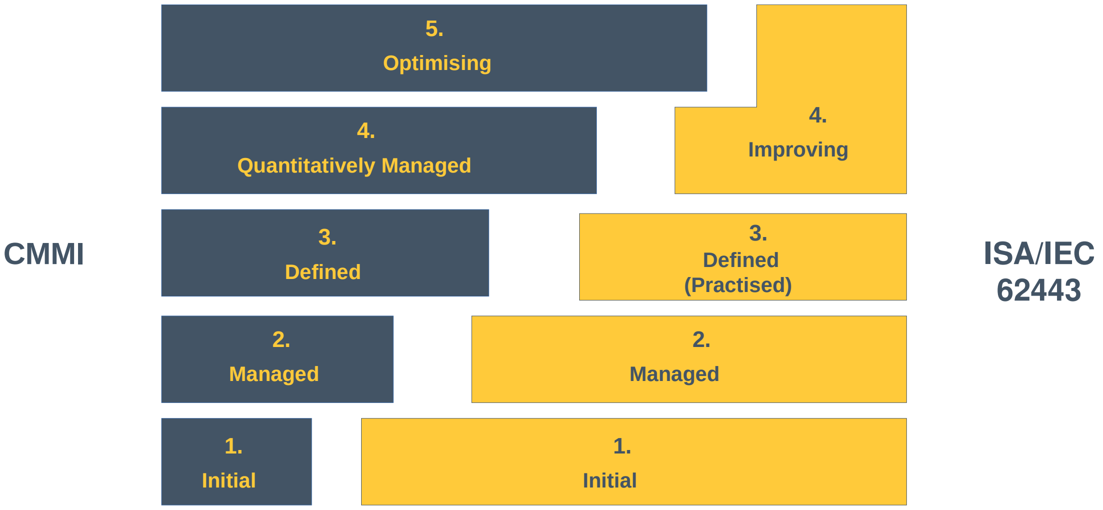
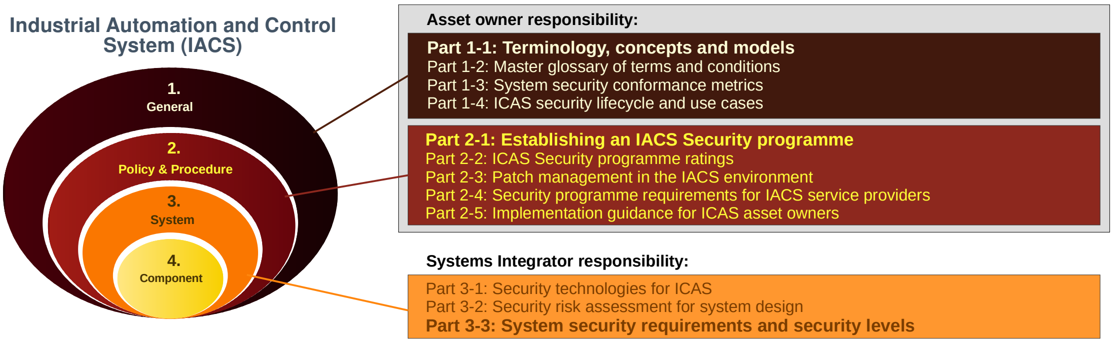


Figure 7: Compare CMMI and ISA/IEC-62433 MLs

The CMMI is an excellent template through which to understand MLs and it is noteworthy that the ISA/IEC 62443 MLs have a lot in common with the CMMI as illustrated in Figure 7. ISA/IEC 62443 MLs are referred to in Parts 2-1, 2-2, 2-4 and 4-1. The first three MLs are identical in focus while the CMMI levels 4 and 5 are combined as a single level 4, Improving in ISA/IEC 62443. Process metrics are used to control effectiveness and performance and continuous improvement.

3 ISA/IEC 62443 Part 3: System



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: Establishing an IACS Security programme
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

Figure 8: ISA/IEC 62443 Part 3: System

The ISA/IEC 62443 Part 3: sets out standards for systems integrators.

3.1 ISA/IEC 62443-3-1: Security technologies for IACS

Part 3-1 is a 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. By following the recommendations of the standard, organisations can significantly reduce their risk of cyberattacks and protect their IACS from harm.

3.1.1 Key requirements

The ISA/IEC 62443-3-1 standard defines a set of security technologies that can be used to protect IACS. These technologies include:

- **Network segmentation**: This technology is used to isolate IACS networks from other networks, making it more difficult for attackers to gain access to IACS.
- **Access control**: This technology is used to control who can access IACS, and what they can do once they are inside.
- **Encryption**: This technology is used to scramble data so that it cannot be read by unauthorised parties.
- **Intrusion Detection and Prevention Systems (IDS/IPS)**: These systems are used to detect and prevent unauthorised access to IACS.
- **Honeypots**: These systems are used to lure attackers into a trap, where they can be identified and neutralised.
- **Security Information and Event Management (SIEM) systems**: These systems are used to collect and analyse security data from IACS and other systems.

The standard also defines a set of security requirements for each of these technologies. These requirements are based on the four security objectives:

- **Availability**: IACS must be available to perform their intended functions at all times.
- **Integrity**: IACS must not be modified in an unauthorised or harmful way.
- **Confidentiality**: The information processed by IACS must be kept confidential.
- **Accessibility**: IACS assets must be accessible to authorised personnel only.

3.2 ISA/IEC 62443-3-2: Security risk assessment for system design

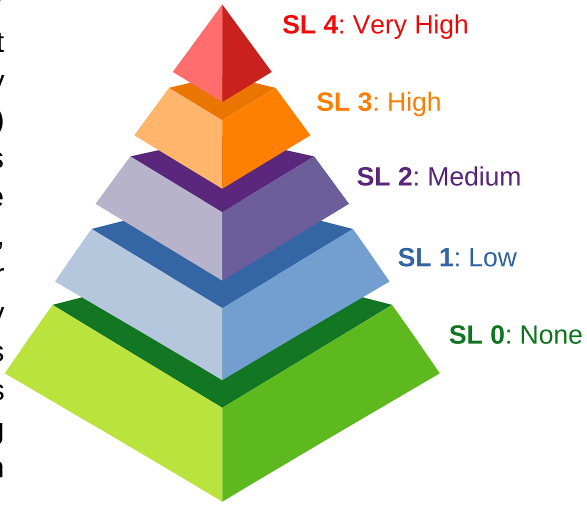
The Part 3-2 technical specification defines the requirements for conducting security risk assessments for IACS. The standard defines a four-step process for conducting security risk assessments for IACS:

- **Identify assets**: The first step is to identify the assets that need to be protected. This includes identifying IACS components, control systems, networks, and data.
- **Analyse threats**: The second step is to analyse the threats that could target IACS. This includes identifying threats from both external and internal sources.
- **Evaluate vulnerabilities**: The third step is to evaluate the vulnerabilities of IACS assets. This includes identifying vulnerabilities in software, hardware, and configuration settings.
- **Assess risk**: The fourth step is to assess the risk to IACS assets. This includes calculating the likelihood and impact of each threat.

The standard also defines a set of security requirements for each step of the security risk assessment process. These requirements are based on the four security objectives defined in Part 3-1, Availability, Integrity, Confidentiality and Accessibility.

3.3 Part 3-3: System security requirements and security levels

Part 3-3 lays out security requirements for IACS with the goal of mitigating cyberattacks. It outlines four increasing stringent security levels, ranging from Security Level (SL) 1 (SL1) (basic) to SL4 (high). Each level specifies security measures for various aspects of the system, including its components, communication, data, and personnel. For instance, SL1 calls for password complexity and access control, while SL4 mandates stricter measures like role-based access control, encryption, and secure coding practices. These are further described later in this document.



3.4 Levels in a Control System

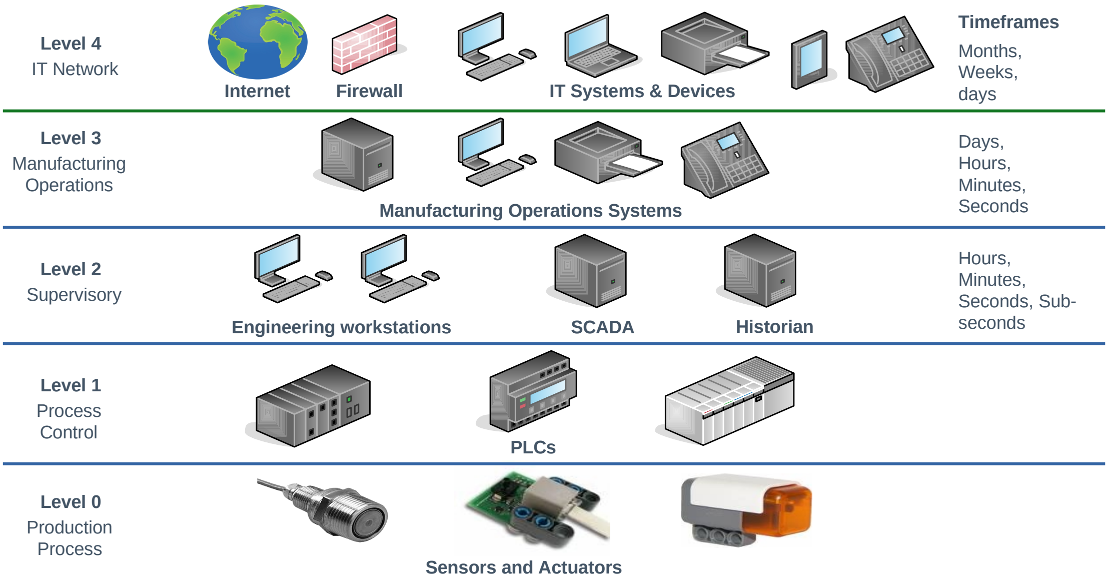


Figure 9: ANSI/ISA-95 Reference Model

As illustrated in Figure 9, and based on the Purdue Enterprise Reference Architecture (PERA) for CIM, the American National Standards Institute (ANSI)/ISA-95 reference model is a hierarchical framework that divides manufacturing operations into five levels:

- **Level 0 - Physical Process**: This level represents the physical devices and equipment that make up the manufacturing process. It includes sensors, actuators, and other machinery used to control and monitor the production process.
- **Level 1 - Manufacturing Execution Systems (MES)**: This level manages and controls the production activities on the shop floor. It includes functions such as production scheduling, order tracking, and quality control.
- **Level 2 - Manufacturing Operations Management (MOM)**: This level integrates the MES with other manufacturing systems, such as Enterprise Resource Planning (ERP) and SCADA. It provides a single point of view for managing and controlling the entire manufacturing process.
- **Level 3 - Business Enterprise Resource Planning**: This level manages the business aspects of manufacturing, such as financials, sales, and distribution. It provides a link between the manufacturing process and the rest of the organisation.
- **Level 4 - Enterprise**: This level represents the overall organisation and its strategic goals. It includes functions such as planning, marketing, and Customer Relationship Management (CRM).

The ANSI/ISA-95 Reference Model provides a common language and framework for exchanging information between these different levels. This allows for real-time data sharing and integration, which can improve efficiency, reduce costs, and improve decision-making.

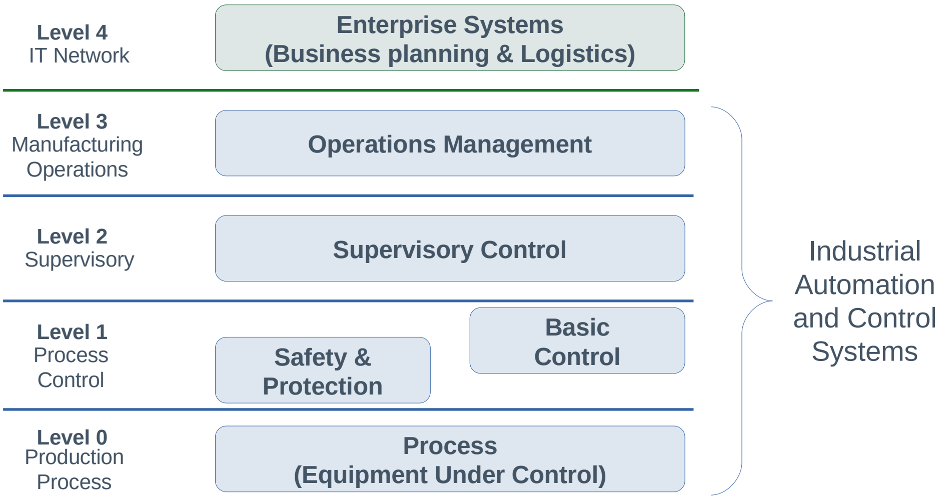


Figure 10: ISA-99 Reference Model

Additionally, the ISA-99 reference model, is a standard framework for securing IACS. Such critical infrastructure systems are used to control and monitor industrial processes, such as manufacturing, power generation, and water distribution. Like ANSI/ISA-95, the ISA-99 Reference Model is based on PERA and divides IACS into four levels or zones:

- **Level 0 – Production Process**: This level interfaces with the physical process through actuators.
- **Level 1 – Process Control**: is the basic control level where the systems overall control takes place. The primary goal of the basic control level is to use controllers to regulate the physical process that interfaces with instrumentation components.
- **Level 2 – Supervisory**: is in charge of interacting and gathering data from the process and control levels so that the operator workstations can monitor and view the control state and field reading of the process. Engineering workstations exist at this level which are used to access controllers setting and programs. Such workstations have a good supply of processors and memory in comparison with the lower levels, which make them more suited for the deployment of security intrusion detection.
- **Level 3 – Manufacturing Operations**: represents the integration of MES with other manufacturing systems, such as ERP and SCADA. It serves as a centralised hub for managing and controlling the entire manufacturing process, from production planning and scheduling to quality control and inventory management.

The ISA-99 Reference Model provides a framework for implementing security controls at each zone of the ICS. It also provides guidance on how to assess and manage the security risks of ICS.

As summarised in Figure 11, the key differences between the ISA-95 Reference Model and the ISA-99 Reference Model are:

Feature	ANSI/ISA-95 Reference Model	ISA-99 Reference Model
Focus	Integration of enterprise and control systems	Security of industrial control systems
Scope	Wider range of applications	Primarily focused on ICS
Approach	Focuses on data exchange and integration	Focuses on security controls and risk management

Figure 11: Comparison between ANSI/ISA-95 and ISA-99

3.5 Security Levels

SLs are defined in ISA/IEC 62443 Part 3-3: "*Security Requirements and Assurance Levels for Industrial Automation and Control Systems (IACS)*." This part of the standard provides a detailed description of the four security levels (SL0, SL1, SL2, and SL3) and the security requirements that must be met for each level. It also provides guidance on how to assess and classify IACS systems and how to implement the necessary security controls.

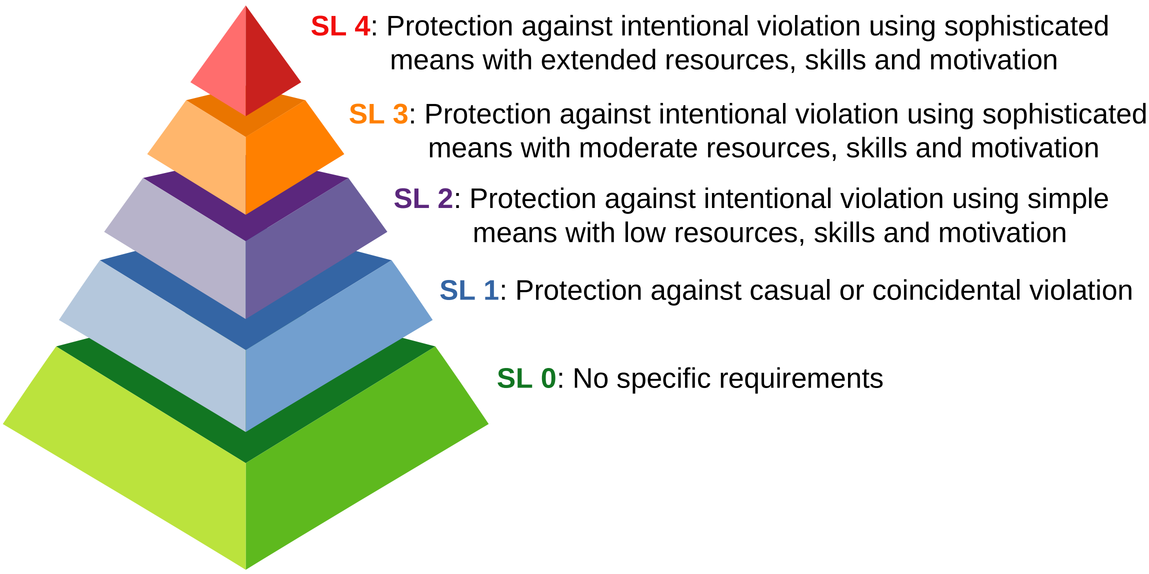

SL 4: Protection against intentional violation using sophisticated means with extended resources, skills and motivation
SL 3: Protection against intentional violation using sophisticated means with moderate resources, skills and motivation
SL 2: Protection against intentional violation using simple means with low resources, skills and motivation
SL 1: Protection against casual or coincidental violation
SL 0: No specific requirements

Figure 12: ISA/IEC 62443 Part 3-3: Security Levels

Additionally Part 4-2, titled "*Technical Security Requirements for IACS Components*", defines the technical requirements for products and each are evaluated through the prism of the four SL. Levels indicate the resistance against different classes of attacker. Increasing SL levels require more stringent controls be in place.

SL	Means	Resources	Skills	Motivation
0	Accidental unintentional	None	None	None
1	Unintentional	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

Figure 13: Security Levels

SL 0: **No specific requirements or security protection necessary**:

- No cyber vulnerabilities.
- No harm can be had from a cyber attack.
- No access controls are mandated.
- Example: Stand-alone non-networked machine.

SL 1: **Protection against casual or coincidental violation**:

- Protection against lax application of security policies.
- This is often attributed to employees rather than external threats.
- Access control mechanisms, auditing and logging, data integrity protection as well as configuration management are mandated.
- Example: Building Heating, Ventilation, and Air Conditioning (HVAC) system.

SL 2: Protection against intentional violation using simple means with low resources, generic skills, and low motivation:

- Attacks that do not require much knowledge of security, the domain, or the particular system under attack by the attacker.
- Access control mechanisms, auditing and logging, data integrity protection, configuration management, Identity Access Management (IAM), vulnerability management, security awareness training are mandated.
- Example: Plant water treatment equipment.

SL 3: Protection against intentional violation using sophisticated means with moderate resources, system specific skills, and moderate motivation:

- Attacks where the instigator has obtained advanced security knowledge, advanced domain knowledge, advanced knowledge of the target system, or any combination of these.
- Examples are exploits in operating systems that are not well known, weaknesses in industrial protocols, specific information about a particular target to violate the security of the system.
- Access control mechanisms, auditing and logging, data integrity protection, configuration management, IAM, vulnerability management, security awareness training, segmentation, security testing, incident response are all mandated.
- Example: Power generation plant.

SL 4: Protection against intentional violation using sophisticated means with extended resources, system specific skills, and high motivation:

- This level is similar to SL3 except that the attacker being even more highly motivated and has extended resources at their disposal.
- Highly likely this level attack is nation state sponsored.
- Access control mechanisms, auditing and logging, data integrity protection, configuration management, IAM, vulnerability management, security awareness training, segmentation, security testing, incident response are all mandated.
- Example: Power generation plant.

3.5.1 SL Controls

The ISA 62443 standard mandates the following controls for Security Level 4 (SL4):

- **Access control mechanisms**: Access control mechanisms should be implemented to restrict access to IACS components and data based on the Principle of Least Privilege (PoLP). This means that users should only be granted the access they need to perform their assigned tasks. Access control mechanisms can include passwords, access tokens, and Role-Based Access Control (RBAC).
- **Auditing and logging**: Auditing and logging mechanisms should be implemented to track user activities and system events. This allows security personnel to monitor for potential anomalies or unauthorised access attempts. Audit logs should be stored securely and reviewed regularly to identify and investigate potential security incidents.
- **Data integrity protection**: Data integrity mechanisms should be implemented to protect data from modification or destruction. This can include data checksums, encryption, and hashing. Data integrity mechanisms should be used to validate data at all stages of the data lifecycle, from input to output.

- **Configuration management**: Configuration management practices should be implemented to ensure that IACS components are configured in a secure manner. This includes the use of change management processes and configuration validation tools. Change management processes should be used to review and approve all changes to IACS configurations. Configuration validation tools should be used to verify that configurations are compliant with security policies.
- **Identity and access management**: IAM should be implemented to manage user identities, permissions, and access to IACS systems. IAM should include features such as user registration, authentication, authorisation, and access control. IAM should be used to ensure that only authorised users have access to IACS systems.
- **Vulnerability management**: Vulnerability management should be implemented to identify and remediate vulnerabilities in IACS systems. Vulnerability management includes scanning IACS systems for vulnerabilities, prioritising vulnerabilities based on their severity, and remediating vulnerabilities in a timely manner.
- **Security awareness training**: Security awareness training should be provided to all IACS users to educate them about security threats and best practices. Security awareness training should cover topics such as password hygiene, social engineering, and phishing attacks.
- **Segmentation**: Segmentation should be implemented to isolate IACS systems from the rest of the network. This can help to prevent unauthorised access to IACS systems and limit the damage that can be caused by a security incident. Segmentation can be implemented using firewalls, Virtual Local Area Networks (VLAN), and other network security technologies.
- **Security testing**: Security testing should be performed on IACS systems to identify and fix vulnerabilities. Security testing can include penetration testing, vulnerability scanning, and code review.
- **Incident response**: Incident response should be in place to respond to and recover from security incidents. Incident response plans should include procedures for identifying, triaging, containing, eradicating, and recovering from security incidents.

3.6 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.

3.7 Zones and Conduits

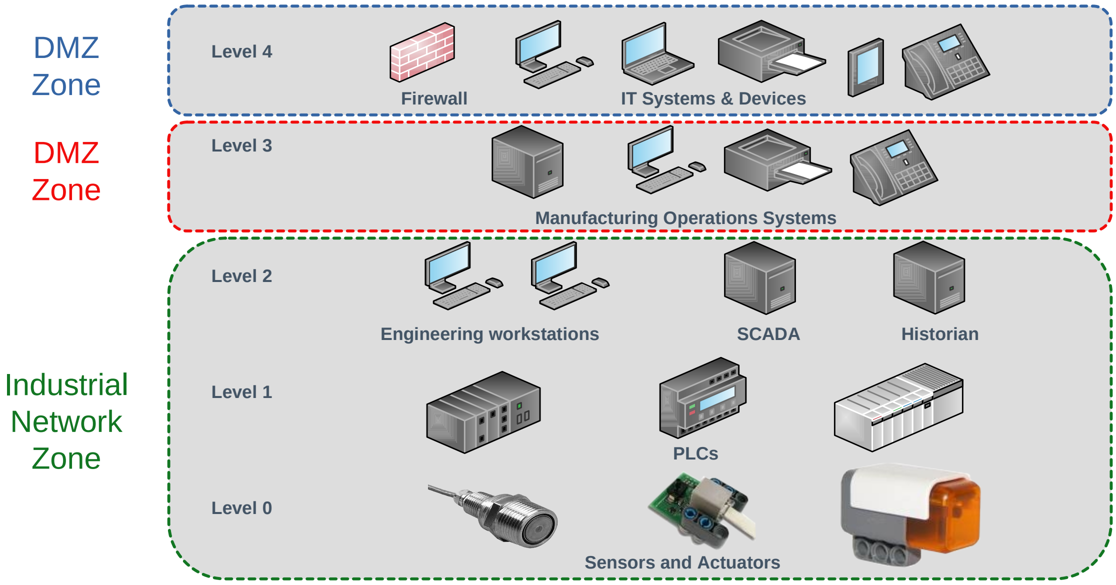


Figure 14: Zones and Conduits

3.7.1 Zones

As illustrated in Figure 14, a zone in the ISA/IEC 62443 context is a logical or physical grouping of IACS assets that share similar security requirements. These assets may include sensors, actuators, PLCs, SCADA systems, enterprise systems, and HMI.

The security requirements for a zone are defined by its SL. The SL indicates the level of protection required for that zone to safeguard the assets within it from unauthorised access, modification, or destruction. The higher the SL, the more stringent the security measures that must be implemented.

3.7.2 Conduits

Conduits are logical or physical groupings of communication channels that connect two or more zones. They enable the flow of information between zones, but also serve as a control point to ensure that only authorised traffic is allowed to pass.

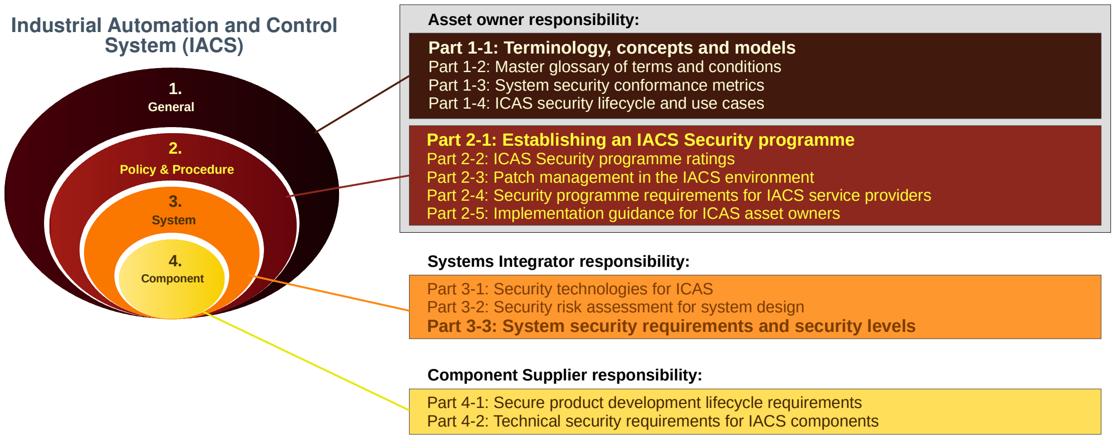
Conduits play a critical role in Defence-in-Depth (DiD) security by providing a barrier between zones with different security levels. They can enforce security policies, such as firewalls, authorisation checks, and encryption, to prevent unauthorised access or data exfiltration.

3.7.3 Zone and Conduit Segmentation

The concept of zones and conduits is essential for implementing effective security in IACS. By dividing the IACS into zones and controlling the flow of information between them, organisations can reduce the attack surface and minimise the impact of potential cyberattacks.

The ISA/IEC 62443 standards provide guidance on how to identify and classify zones, define SLs, and implement appropriate security controls for conduits. This segmentation approach helps organisations to protect their critical IACS assets and ensure the safety, security, and reliability of their operations.

4 ISA/IEC 62443 Part 4: Component



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: Establishing an IACS Security programme
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

Figure 15: ISA/IEC 62443 Part 4: Component

The ISA/IEC 62443 Part 4: sets out standards for systems integrators.

4.1 ISA/IEC 62443-4-1: Secure product development lifecycle

Part 4-1 is a technical specification that defines 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.

4.1.1 Key requirements

The standard defines a set of requirements for implementing a secure product development lifecycle for IACS. These requirements are divided into seven main categories:

- **Planning**: Organisations must establish a security policy and plan for their product development lifecycle.
- **Design**: Organisations must design their products with security in mind.
- **Development**: Organisations must develop their products according to secure coding practices.
- **Testing**: Organisations must test their products to identify and fix security vulnerabilities.
- **Deployment**: Organisations must deploy their products securely.
- **Operation**: Organisations must operate their products securely.
- **Decommissioning**: Organisations must decommission their products securely.

The standard also defines a set of security requirements for each of these phases of the product development lifecycle. These requirements are based on the four security objectives defined in Part 3-1, Availability, Integrity, Confidentiality and Accessibility.

4.2 ISA/IEC 62443-4-2: Security requirements for components

Part 4-2 is a technical specification that defines the security requirements for components of IACS. The standard is to 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.

4.2.1 Key requirements

The ISA/IEC 62443-4-2 standard defines a set of security requirements for IACS components. These requirements are divided into five main categories:

- **Identification and classification**: Organisations must identify and classify their IACS components based on their security criticality.
- **Security policy**: Organisations must implement a security policy for their IACS components.
- **Vulnerability management**: Organisations must manage the vulnerabilities of their IACS components.
- **Protection against unauthorised access**: Organisations must protect their IACS components against unauthorised access.
- **Security updates**: Organisations must periodically update their IACS components with security patches.

The standard also defines a set of security constraints.

4.2.2 Threat Modelling

A key processes of the SDL is threat modelling. This is a systematic process to identify data flows, trust boundaries, attack vectors, and potential threats to the IACS. 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.

4.3 Common Cyber Security Constraints

In part 4.2 of the ISA/IEC 62443 series there are four CCSC defined:

- **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. For this purpose, the countermeasures must be described in the documentation of the component.
- **CCSC 3**: requires that the PoLP is applied in the component. This means that users are given the minimum levels of access permissions required to perform their job functions.
- **CCSC 4**: requires that the component is developed and supported by ISA/IEC 62443 Part 4-1 compliant development processes.

5 Dependencies

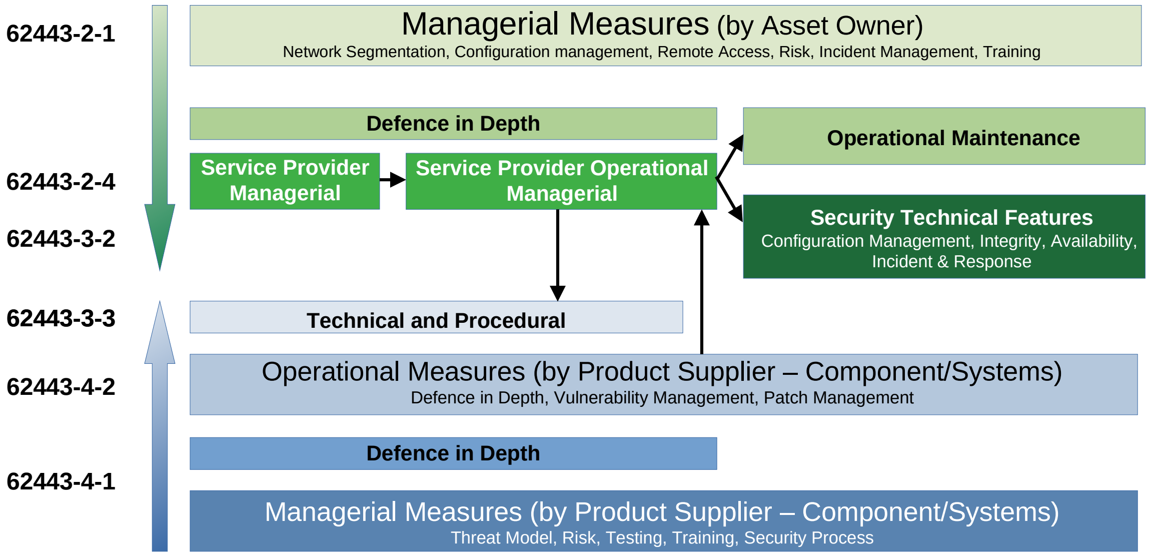

62443-2-1
62443-2-4
62443-3-2
62443-3-3
62443-4-2
62443-4-1
Managerial Measures (by Asset Owner)
Network Segmentation, Configuration management, Remote Access, Risk, Incident Management, Training
Defence in Depth
Operational Maintenance
Service Provider Managerial
Service Provider Operational Managerial
Security Technical Features
Configuration Management, Integrity, Availability, Incident & Response
Technical and Procedural
Operational Measures (by Product Supplier – Component/Systems)
Defence in Depth, Vulnerability Management, Patch Management
Defence in Depth
Managerial Measures (by Product Supplier – Component/Systems)
Threat Model, Risk, Testing, Training, Security Process

Figure 16: Dependencies

Figure 16 represents the dependencies in the ISA/IEC 62443 series of standards where three levels of security: managerial, operational, and technical, are illustrated.

- **Managerial measures**: are the highest level of security and are responsible for setting the overall security policy for an IACS. They include things like risk assessment, incident management, and training.
- **Operational measures**: are responsible for implementing the security policy and ensuring that it is followed. They include things like network segmentation, configuration management, and remote access.
- **Technical measures**: are the lowest level of security and are responsible for protecting the IACS from physical and cyber threats. They include things like firewalls, intrusion detection systems, and access control lists.

Figure 16 also illustrates that there are three different types of entities that are responsible for security in an IACS: asset owners, service providers, and product suppliers.

- **Asset owners**: are the organisations that own and operate IACS. They are responsible for developing and implementing the security policy for their IACS.
- **Service providers**: are organisations that provide integration and maintenance services for IACS. They are responsible for implementing the security policy and ensuring that it is followed.
- **Product suppliers**: are organisations that develop and sell IACS products. They are responsible for designing and implementing security features into their products.

The diagram is a useful tool for understanding the different levels of security for IACS and the roles and responsibilities of different entities in securing IACS.

6 Summary

The ISA/IEC 62443 series of standards, guidelines is a comprehensive set of security standards and guidelines for the protection of IACS. The standards are developed by ISA and IEC, and are widely recognised as the authoritative source of guidance on IACS security. The standards cover a wide range of topics, including:

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

By following the recommendations of the ISA/IEC 62443 standards, organisations can protect their IACS from a wide range of cyberattacks. The standards are particularly important for organisations that operate critical infrastructure, such as power plants, water treatment facilities, and manufacturing plants. This leads to reduced risk of cyberattacks, improved resilience, enhanced compliance, enhanced operational efficiency, and reduced costs

Overall, the ISA/IEC 62443 standards are a valuable resource for organisations that want to protect their IACS from cyberattacks. By following the recommendations of the standards, organisations can create a more secure system that is resistant to cyberattacks.

7 Example use of ISA/IEC 62443

7.1 IACS Environment

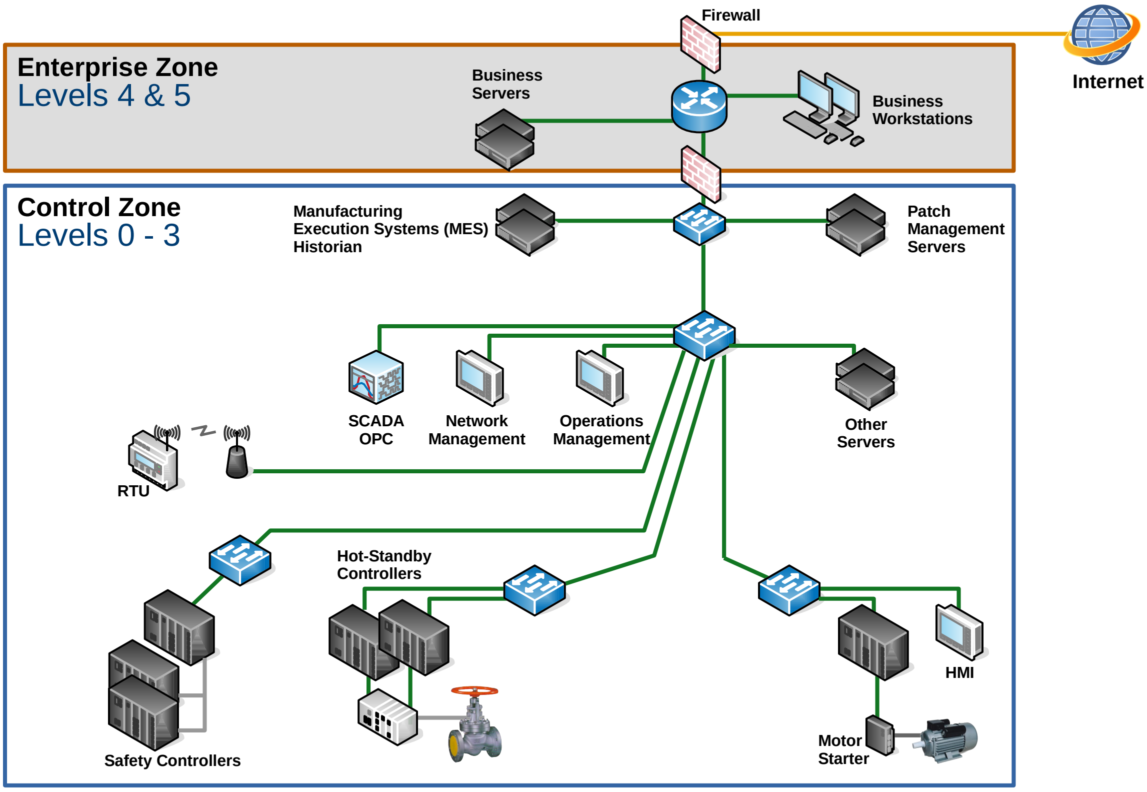


Figure 17: Example IACS

SCADA Open Platform Communications (OPC): a communication protocol for secure data exchange in SCADA systems.

The diagram, in Figure 17, illustrates an IACS at SL0, before ISA/IEC 62443 standard are applied.

7.2 Security Level 1

	Requirement	Actions to satisfy requirements
1	Control system can authenticate and authorise human users. User accounts can be created and managed. Configurable password strength. Track unsuccessful login attempts.	End user accounts created in devices or centralised authentication server.
2	Control system can authenticate and authorise wireless users.	Mobile devices and network infrastructure authenticates users.
3	Control system shall provide the ability to monitor and control access from untrusted networks.	Firewalls monitor traffic from untrusted networks.
4	Control system shall be able to restrict code embedded in e-mail or on storage media.	ePolicy Orchestrator (ePO) server can restrict interactions with mobile devices.
5	Control systems shall provide the capability to generate audit records.	Audit records/logs generated by equipment.
6	Control system shall protect the integrity of transmitted information.	Equipment supports encrypted protocols, robust check sums/hashing.
7	Control system shall detect, prevent, and report the effects of malicious code.	Application whitelisting enabled on end devices.
8	Control system shall protect the confidentiality of information at rest or in transit.	Equipment supports user names and passwords for authorisation.
9	Control system shall segment networks and protect boundaries.	Firewalls segment networks and protect boundaries.
10	Control system shall be able to prevent messages being received from external users or systems.	Firewall can filter messages from external networks.
11	The control system shall provide the capability to support partitioning of data, applications, and services based on criticality to implement a zoning model.	Networks should be segmented using zone and conduit modelling.
12	Control system shall operate in degraded mode during DoS event.	Network elements (switches, routers, etc.) support rate limiting.
13	Prohibit unnecessary functions, ports, protocols, and services.	IACS devices have the ability to disable unnecessary capabilities.
14	Control system shall conduct backup of user and system level information.	Backup files available within individual devices.

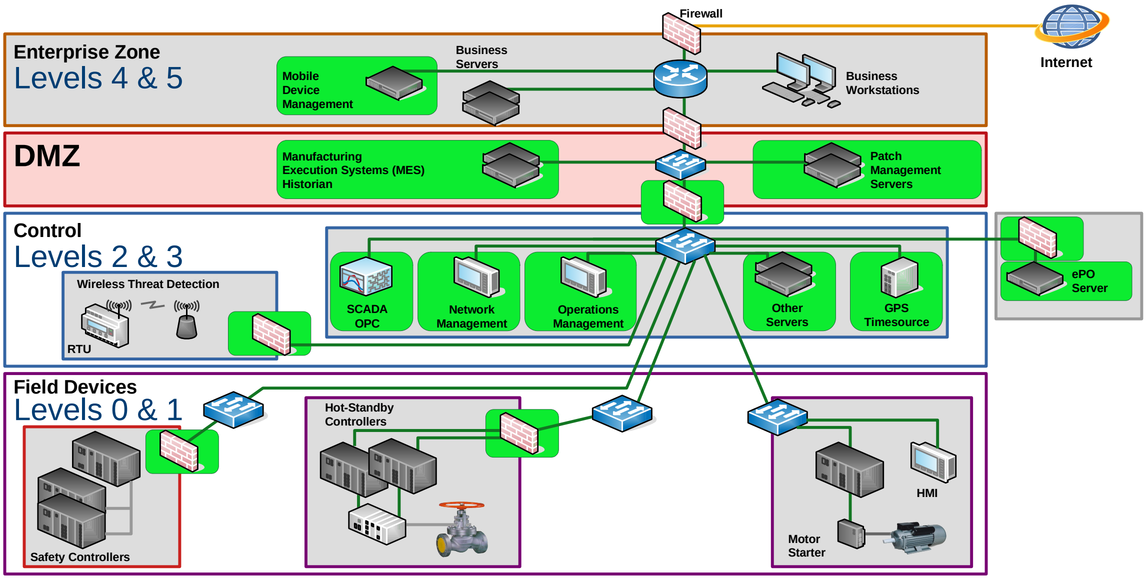


Figure 18: IACS with SL1 controls applied

Figure 18 shows a more secure configuration with SL1 requirements of ISA/IEC 62443 applied.

- **Additional security apparatus added**: Examples such as adding an ePolicy Orchestrator (ePO) server, a centralised software platform used to manage and enforce security policies across an entire network, as well as network segmentation, increase the overall security levels. Firewalls are added at gateways to various segments thereby isolating any vulnerabilities within the segment.
- **Evolution beyond basic needs**: Some actions address concerns not explicitly mentioned in the initial requirements, such as DoS resilience and data zoning.

7.3 Security Level 2

	Requirement	Actions to satisfy requirements
1	The control system shall authenticate and authorise software processes and devices.	Software and devices authenticate using certificates.
2	The control system shall authenticate human and software users engaged in wireless communications.	Mobile devices and network infrastructure authenticates users against centralised authentication server.
3	The control system shall support standard Public Key Infrastructure (PKI) and certificate-based authentication if used.	Certificate authority added in control network to issues certificates.
4	The control system shall be able to deny access requests from untrusted networks unless approved by an assigned role.	Feature enabled in end devices.
5	The control system shall enable authorised users to define and modify mapping of permission to roles.	Roles and permissions enabled in devices or unified account management appliance.
6	The control system shall employ malicious code protection at all entry and exit points.	Network (IDS) support provides malicious code protection. Centralised server implemented with remote Network Intrusion Detection (NID) nodes protect networks.
7	The control system shall protect the integrity of sessions.	Equipment supports encrypted protocols.
8	The control system shall protect the audit information.	Event server employed as centralised repository for equipment records. End devices forward records to event server.
9	The control system shall protect confidentiality in remote access traversing an untrusted network.	Virtual Private Network (VPN) initiated from firewall secures remote access connections.
10	The control system shall provide the capability to physically segment control system networks from non-control system networks.	Communication from critical systems transported over different networks than non-critical systems.
11	The control system shall report list of installed components with associated properties.	Data recorded in repository - capability can be provided by IDS.

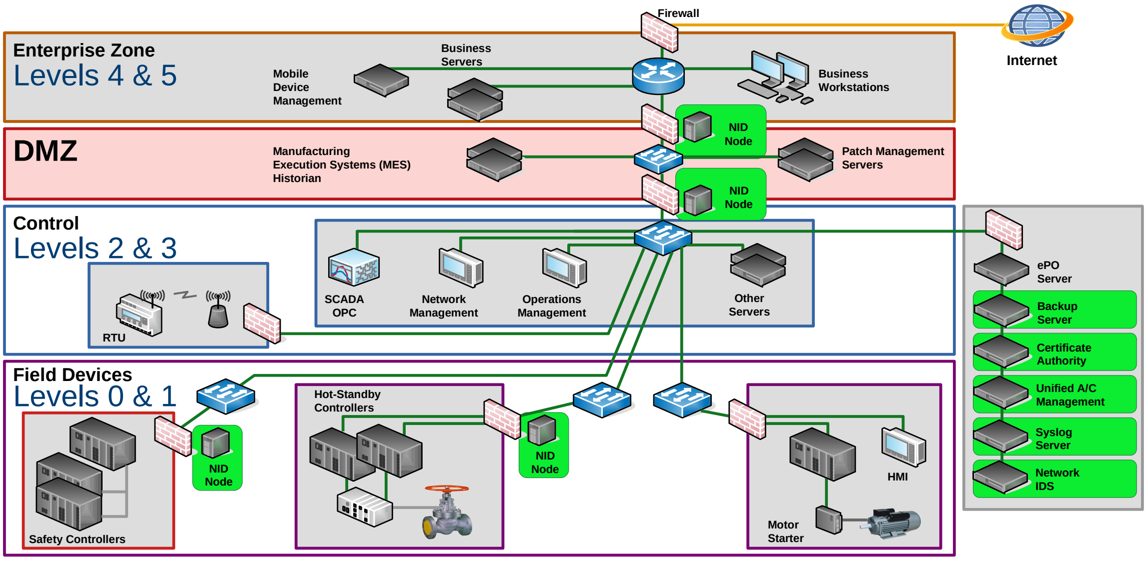


Figure 19: IACS with SL2 controls applied

SL2 controls add at the network and device level. At the network level the following additions were made:

- **Network Intrusion Detection (NID)**: devices focusing on monitoring network traffic within IACS to identify and potentially respond to malicious activity, were added at the DMZ firewalls and at the gateway to various segments. These form a key security component, particularly at higher security levels such as SL2 and SL3.
- Servers: Additional Backup, Logging and Security functions are added at the Control levels.

Overall, the additions for SL2 control add redundancy, segmentation, and security to the network. This helps to improve the availability, reliability, and security of the control system.

7.4 Security Level 3

	Requirement	Actions to satisfy requirements
1	The control system shall support multi-factor authentication for untrusted interfaces.	Feature enabled through centralised account management and end devices.
2	The control system shall uniquely identify and authenticate software processes.	Feature supported through certificate authority. Secure protocols can also be utilised.
3	The control system shall support unified account management.	Unified account management enabled through centralised account management.
4	The control system shall protect private keys using hardware mechanisms.	Secure element in IACS equipment.
5	The control system shall identify and report unauthorised wireless devices	Identification of unauthorised wireless devices through the addition of wireless threat detection device.
6	The control system shall verify the integrity of mobile code before allowing execution.	Mobile code integrity verified from the ePO server and certificate authority.
7	The control system shall provide a centrally managed system wide audit trail.	End devices forward log files to SIEM server.
8	The control system shall synchronise internal system clock at configurable frequency.	GPS time source added to network.
9	The control system shall support cryptographic mechanisms to recognise changes to information during communication.	Enabled through the use of secure protocols.
10	The control system shall centrally manage malicious code protection mechanisms.	Malicious code is protected via the ePO server and SIEM server. All detected issues are forwarded to the SIEM server.
11	The control system shall support automated backup based on configurable frequency.	Automated backup function is supported in the backup server.
12	The control system shall report the current security settings on end devices.	The ePO Server coupled with network management systems report security settings.

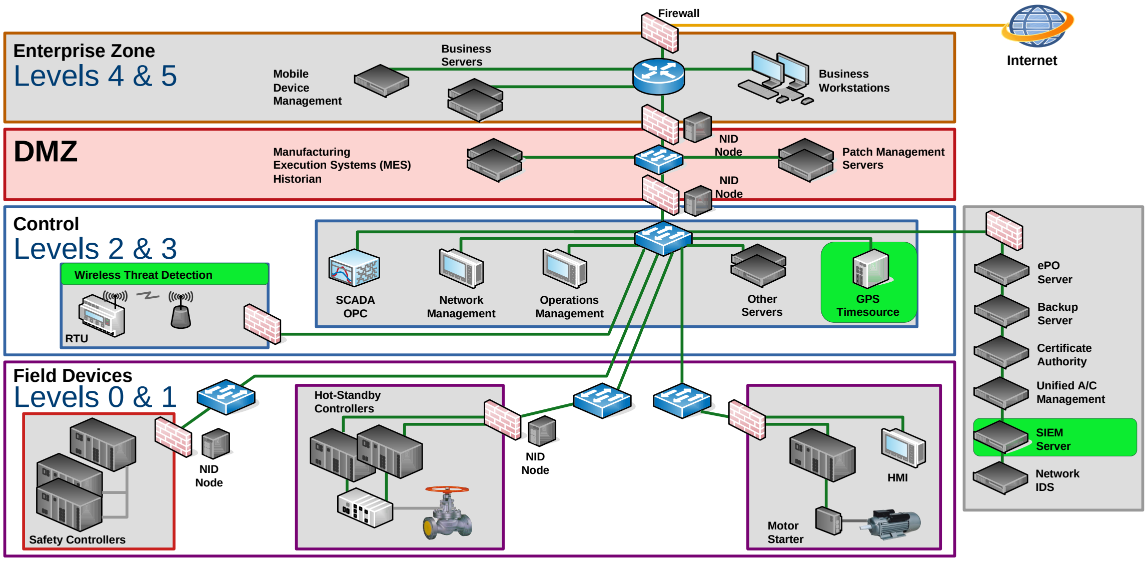


Figure 20: IACS with SL3 controls applied

Additions illustrated, in Figure 20, for SL3 controls at the network level are threat detection on wireless networks, a Global Positioning System (GPS) Timesource function is independent of network connectivity. This proves invaluable in scenarios where network outages or disruptions could compromise time accuracy. GPS time signals are inherently difficult to manipulate due to their origin and encryption used by most systems. This adds an extra layer of security compared to network-based time sources, which can be susceptible to cyberattacks aimed at disrupting time synchronisation.

A SIEM Server is also added which acts as a security information and event management hub, collecting and analysing data from various sources to detect and respond to security threats across your network. In short, it helps you see and stop security issues before they cause harm.

8 Industrial Cybersecurity Technology & Solutions

- **Technology Concerns**
    - Network Segmentation
    - Lack of system hardening
    - Weak access control
    - Insufficient levels of Identity Management
    - Insufficient logging and monitoring
    - OT/Industrial IoT (IIoT) Device-level security (L0/1)
    - Vulnerabilities, Product Security and the Supply Chain
    - Industrial Cloud Security

- **Business Concerns**
    - Collaboration and Risk
    - Weak Governance
    - Security awareness and training
    - Third party management
    - Incident response planning

9 Exercise: Exploring OTSec with ISA/IEC 62443

Objective

To grasp the application of ISA/IEC 62443 in securing IACS and understand its key concepts through research and group discussions.

Part 1: Individual

- **Assigned Section**: Each student will receive a section of ISA/IEC 62443 (Assigned by the lecturer).
- **Research and Summarise**: Conduct in-depth research on the assigned section, summarising its key components, requirements, and best practices. Focus on aspects relevant to understanding and implementing robust IACS security.
- **Prepare Presentation**: Develop a concise presentation with visuals explaining the core aspects of your assigned section within a broader context of ISA/IEC 62443. This will be incorporated into a final presentation on part 3.

Part 2: Group

- **Shared Understanding**: Present your assigned section to the group, ensuring everyone gains a solid foundation in all areas of ISA/IEC 62443.
- **Comparative Analysis**: Compare and contrast different sections, highlighting overlapping aspects and how they work together to create a comprehensive security framework.
- **Case Study Application**: Choose a real-world IACS scenario (e.g., water treatment plant, power grid) and discuss how you would apply various elements of ISA/IEC 62443 to secure it. This can involve threat identification, risk assessment, control implementation, and incident response strategies.

Part 3: Written Report, Presentation and Video

Create a written report, presentation and video that incorporates your findings from from part 1, plus

- **Your understanding of the outputs from part 2**. Note: This is your specific understanding, this is not a shared set of slides from the group work. You must also indicate your specific contributions to the group work (initials in the margin i.e. [OB]
- **Comparative Analysis with Other Frameworks**: Compare and contrast ISA/IEC 62443 with other cybersecurity frameworks such as NIST Cybersecurity Framework, ISO 27001, etc.., identifying similarities and differences in their approaches to protecting critical infrastructure.
- **Presentation and Video**: Create a video explaining ISA/IEC 62443 using the presentation as a foundation.

Assessment

- **Group Participation**: Active involvement in discussions, insightful comparisons, and contribution to the case study analysis.
- **Individual Written Report**: A concise report summarising key learnings, comparisons, and insights gained from the exercise.
- **Individual Presentation**: Clarity, accuracy, and depth of understanding of the assigned section of ISA/IEC 62443.
- **Individual Video**: Ensure the video is engaging, informative, and meets the learning objectives.

10 Bibliography

[1] ISA/IEC 62443, ‘Industrial communication networks - IT security for networks and systems’. International Society of Automation/International Electrotechnical Commission, Jul. 20, 2009.

This page is intentionally blank