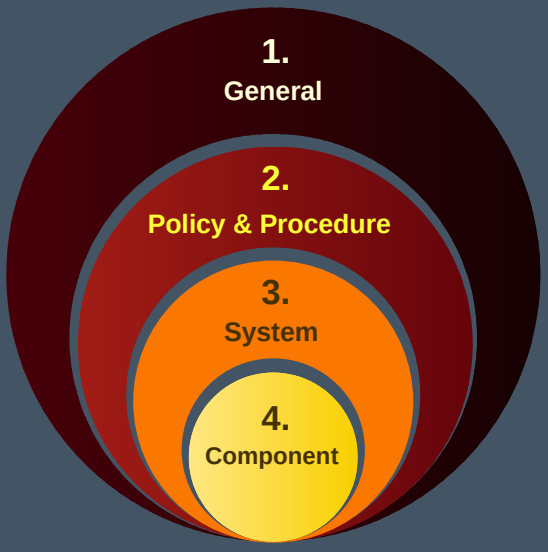
Cybersecurity for Industrial Networks

Topic 3.1
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

This page is intentionally blank

1 Introduction

1.1 Learning Objectives

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

- understand the importance of securing Industrial Automation and Control Systems (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.

1.2 Why Secure IACS?

IACS are physical-cyber systems, the impact of a cyberattack could be quite severe. The consequences of a cyberattack on an IACS include, but are not limited to:

- Endangerment of public or employee safety or health
- Damage to the environment
- Damage to the Equipment Under Control (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.

1.3 How are IACS different from IT Systems?

The priority of security when it comes to the enterprise Information Technology (IT) systems and networks is the prevention of unauthorised access often termed the Confidentiality, Integrity, Availability (CIA) triad. While the priority of an OT in IACS is the safe, continuous availability of the system. For example, while it may be acceptable for a computer in an enterprise IT environment to be offline while the Operating System (OS) carries out a software update, this is almost certainly not acceptable in an OT IACS.

Security Objective	Description	Priority
Safety	IACS must not cause harm to people, property, or the environment.	Overarching
Availability	IACS must be available to perform their intended functions at all times.	Highest
Integrity	IACS must not be modified in an unauthorised or harmful way.	High
Confidentiality	Sensitive information processed by IACS must be kept confidential.	Medium
Accessibility	IACS assets must be accessible to authorised personnel only.	Lowest

Figure 1: IACS Security Priorities

As illustrated in Figure 1, Safety of OT is the overarching goal of cybersecurity because IACS are used to control critical infrastructure, such as power plants, water treatment systems, and manufacturing plants. If IACS are not secure, they could be used to cause serious safety hazards.

After safety the highest priority is the Availability of the plant process and production capability as well as the Integrity of the system. Following Availability is Integrity, Confidentiality, and Accessibility.

While Confidentiality is important in the OT context, it is not the highest priority as it is in IT systems. Priority in OT is therefore abbreviated into Safety, Availability, Integrity, Confidentiality, Accessibility (SAICA).

Cyber threats come from many vectors, for example, internal employees many unintentionally or intentionally contribute to an attack as well as external actors, such as hacktivists, cybercriminals, organised crime, and nation-state sponsored attackers.

Attacks maybe in the form of ransomware, malware, directed remote access attacks, and coordinated attacks on IACS as well as supporting infrastructure such as the company enterprise networks and 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.

1.4 How to Secure IACS?

To counter OT threats the implementation of a standard such as the ISA/IEC 62443 [1] to create a Cyber Security Management System (CSMS), which prevent or lessen the risk of cyberattacks by planning, implementing procedures and creating polices and processes over the following basic steps:

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

2 The Purdue model for IACS

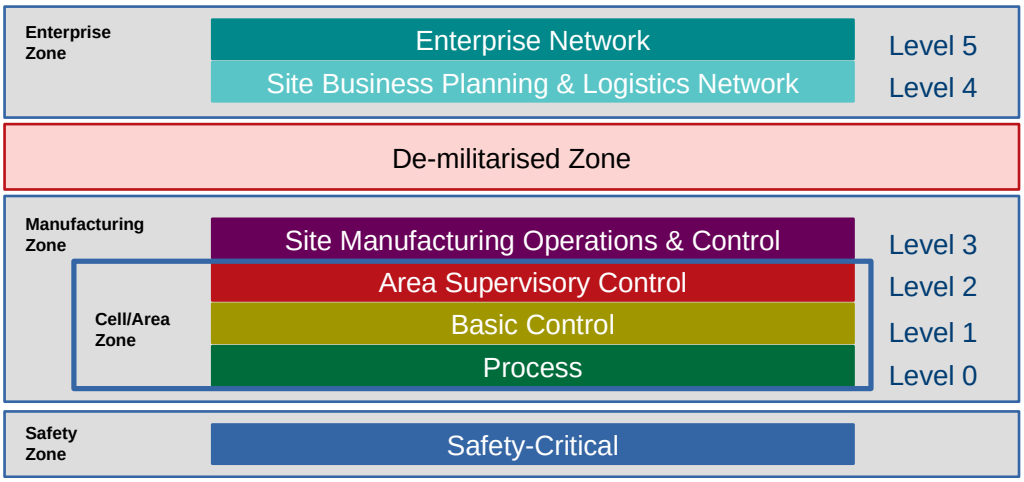


Figure 2: Purdue Model

The Purdue model, or Purdue Enterprise Reference Architecture (PERA) model, for Computer-Integrated Manufacturing (CIM) is used as a concept model for IACS network segmentation. It is an industry adopted reference model that shows the interconnections and interdependencies of all the main components of a typical IACS. The IACS is divided into three zones and six levels as illustrated in Figure 2.

2.1 The Enterprise Zone

The enterprise zone is the part of the IACS where business systems such as Enterprise Resource Planning (ERP) exist. Here, tasks such as scheduling and supply chain management are performed. The enterprise zone can be subdivided into two levels, Level 5 – Enterprise Network and Level 4 Site business and logistics.

2.1.1 Level 5 - Enterprise network

The systems on the enterprise network are typically positioned at a corporate level and span multiple facilities or plants. They take data from subordinate systems from the individual plants and use the accumulated data to report on the overall production status, inventory, and demand. However, technically the enterprise zone is not part of the IACS and it relies on connectivity with the IACS networks to feed the data that drives business decisions.

2.1.2 Level 4 - Site business planning and logistics

Level 4 houses the IT systems that support the production process in a plant of a facility. These systems report production statistics such as uptime and units produced for corporate systems. It takes orders and business data from the corporate systems to be distributed among the OT or IACS systems. Systems typically found in level 4 include database servers, application servers (web, report, Manufacturing Execution Systems (MES)), file servers, email clients, supervisor desktops, etc...

2.2 Industrial Demilitarised Zone

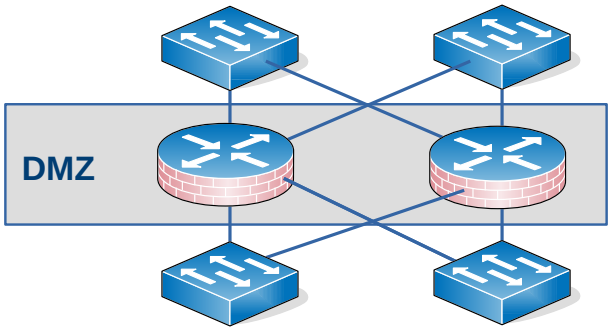


Figure 3: Industrial DMZ

Between the enterprise zone and systems and the Industrial zone lies the Industrial Demilitarised Zone (IDMZ). Much like a traditional (IT) DMZ, the OT-oriented IDMZ facilitates securely connect networks with different security requirements.

The IDMZ is the result of the efforts taken to create security standards such as the NIST Cyber Security Framework (CSF) [2] and North American Electric Reliability Corporation - Critical Infrastructure Protection (NERC CIP) [3].

The IDMZ is an information sharing layer between the business or IT systems in levels 4 and 5 and the production or OT systems in levels 3 and lower. By preventing direct communications between IT and OT systems and having a broker service in the IDMZ to relay the communications, an extra layer of separation and inspection is added to the overall architecture. Systems in the lower layers are not directly exposed to attacks or compromise. If something were to compromise a system at some point in the IDMZ, the IDMZ could be shutdown, the compromise could be contained, and production could continue.

Systems typically found in the Industrial Demilitarised Zone include (web) proxy servers, database replication servers, domain controllers, etc...

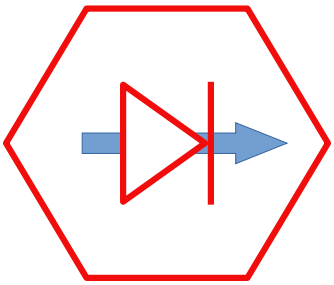


Figure 4: Data Diode

For certain, highly sensitive, Industrial Zones a Data Diode is used in lieu of a firewall. A Data Diode is a hardware-based one-way Ethernet connection between two networks. They permit the movement of data from the Industrial Zone to the Enterprise Zone but do not allow traffic to pass the other direction.

2.3 The Manufacturing Zone

The manufacturing zone is the heart of the IACS. It is the zone where the manufacturing process and devices exist. The manufacturing zone is subdivided into four sub-levels, Level 3 Site operations, Level 2 Area Supervisory control, Level 1 Basic control and Level 0 the process.

2.3.1 Level 3 - Site operations

Level 3 is where systems that support plant wide control and monitoring functions reside. At this level, the operator is interacting with the overall production systems. Consider centralised control rooms with Human Machine Interfaces (HMI) and operator terminals that provide an overview of all the systems that run the processes in a plant or facility. The operator uses these HMI systems to perform tasks such as quality control checks, managing uptime, and monitoring alarms, events, and trends.

Level 3, site operations, is also where the OT systems that report back up to IT systems in level 4 exist. Systems in the lower levels send production data to data collection and aggregation servers at this level, which can then send the data to higher levels or can be queried by systems in higher levels.

Systems typically found in level 3 include database servers, application servers (web and report), file servers, domain controllers, HMI servers, engineering workstations, etc..

2.3.2 Level 2 - Area supervisory control

Many of the functions and systems in level 2 are the same as for level 3 but targeted more toward a smaller part or area of the overall system. In this level, specific parts of the system are monitored and managed with HMI systems. Consider a single machine or skid with a touch screen HMI to start or stop the machine or skid and see some basic running values and manipulate machine or skid-specific thresholds and set points.

Systems typically found in level 2 include HMIs (standalone or system clients), supervisory control systems such as a line control Programmable Logic Controllers (PLC), engineering workstations, etc...

2.3.3 Level 1 - Basic control

Level 1 is where all the controlling equipment exists. The main purpose of the devices in this level is to open valves, move actuators, start motors, etc... Typically found in level 1 are PLCs, Variable Frequency Drives (VFD), dedicated Proportional-Integral-Derivative (PID) controllers, etc... Although a PLC can be found in level 2, its function would be of a supervisory nature instead of as a controller.

2.3.4 Level 0 - Process

Level 0 is where the actual process equipment that are used for controlling and monitoring from the higher levels exist. EUC, level 1 is where devices such as motors, pumps, valves, and sensors that measure speed, temperature, or pressure can be found. As level 0 is where the actual process is performed and where the product is made, it is imperative that things run smoothly and uninterrupted. The slightest disruption in a single device can cause mayhem for all operations.

3 The ISA/IEC 62443 Standard

The ISA/IEC 62443 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.

3.1 Who are the ISA & IEC

Initially, the International Society of Automation (ISA) 99 (ISA-99) committee considered IT standards and practices for use in the IACS. However, it was soon found that this was not sufficient to ensure the safety, integrity, reliability, and security of an IACS.

The ISA and the International Electrotechnical Commission (IEC) have addressed the gap to improve the cybersecurity of IACS via the ISA/IEC 62443 standard.

The goal of the IEC/ISA-62443 series is to improve the safety, reliability, integrity and security of IACS using as risk-based, methodical and complete process throughout the entire lifecycle.

3.2 Core principles of ISA/IEC 62443

The ISA/IEC 62443 series is based on four core principles:

- **Security by design**: IACS security should be considered from the earliest stages of system development and should be integrated into the overall design and architecture.
- **Security by default**: Default configurations should be secure and should not require additional configuration to be secure.
- **Security throughout the lifecycle**: Security should be maintained throughout the entire lifecycle of the IACS, from design and development to operation and maintenance.
- **Security risk management**: Security should be based on a risk-management approach that considers the specific threats, vulnerabilities, and consequences of a security breach.

3.3 Structure of the ISA/IEC 62443 series

The ISA/IEC 62443 series consists of four parts:

Part 1: General

- **Part 1-1**: 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 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 aspects for IACS service providers
- **Part 2-5**: Implementation guidance for IACS asset owners

Part 3: System

- **Part 3-1**: Security architecture and components
- **Part 3-2**: Security capabilities and requirements for components
- **Part 3-3**: System security requirements and security levels

Part 4: Component

- **Part 4-1**: Security requirements for applications
- **Part 4-2**: Security requirements for system integration and communication.

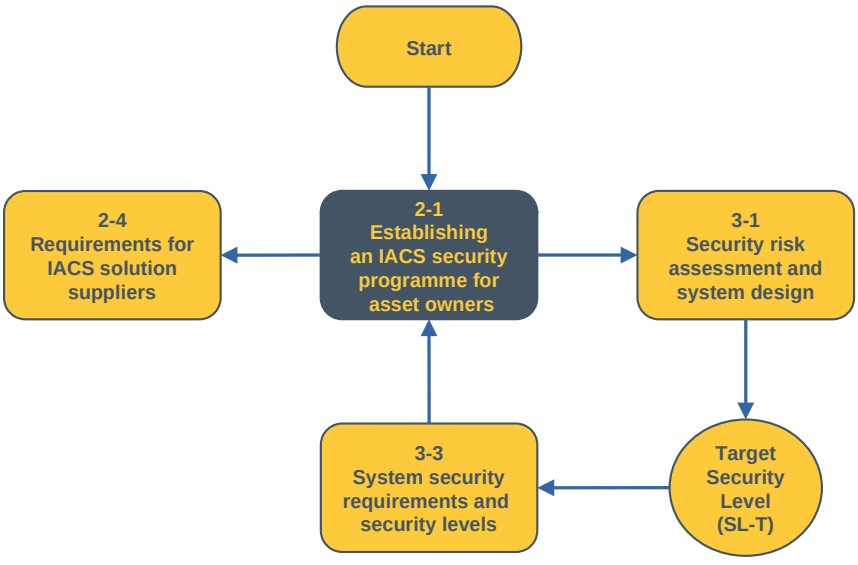


Figure 5: Structure of the ISA/IEC 62443 series

3.4 Benefits of implementing ISA/IEC 62443

The ISA/IEC 62443 series provides several benefits to organisations that implement it, including:

- **Reduced risk of cyber attacks**: By following the standards, organisations can significantly reduce the risk of cyber attacks on their IACS.
- **Improved resilience**: Secured IACS are more resilient to cyber attacks, and are less likely to experience downtime or disruptions.
- **Enhanced compliance**: The standards are aligned with many national and international cybersecurity regulations.
- **Improved operational efficiency**: Secured IACS can operate more efficiently and reliably.
- **Reduced costs**: By preventing cyber attacks, organisations can save money on remediation, lost productivity, and reputational damage.

Overall, the ISA/IEC 62443 series is a valuable resource for organisations that want to secure their IACS. The standards provide a comprehensive and practical approach to cybersecurity, and can help organisations to protect their critical infrastructure from cyber threats.

3.5 Holistic Security Concept

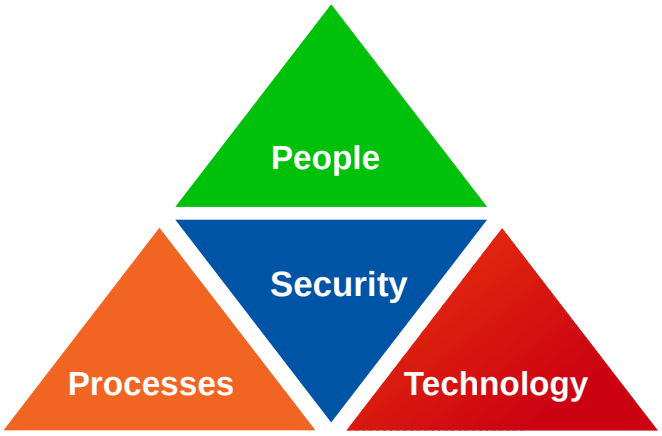


Figure 6: Holistic Security

The scope of the ISA/IEC 62443 series is the Security of IACS. The holistic security concept, illustrated in Figure 6, demonstrates that security relies on the alignment of people, process and technology. In the case of an asset owner or systems integrator this in the main involved people and processes while the component supplier must also concern themselves with the technology.

3.6 Key Roles

Role	Responsibilities
Asset Owner	Define security requirements, develop and implement security policies and procedures, conduct regular security assessments and audits, investigate and respond to security incidents
Maintenance Service Provider	Perform routine maintenance tasks, address cybersecurity vulnerabilities, provide training to operators, update firmware and software
Integration Service Provider	Design and deploy security solutions, configure and manage security devices, test and verify security controls, document security procedures
Product Supplier	Integrate security into the product design, provide cybersecurity documentation, test and validate security features, provide vulnerability management and security updates

Figure 7: ISA/IEC 62443 Key Roles

The ISA/IEC 62443 series of standards defines four key roles:

The Asset Owner

The asset owner is the organisation that has the ultimate responsibility for the security of its IACS. This includes:

- Defining security requirements
- Developing and implementing security policies and procedures
- Conducting regular security assessments and audits
- Investigating and responding to security incidents

Maintenance Service Provider

The maintenance service provider is responsible for maintaining and supporting the IACS. This includes:

- Performing routine maintenance tasks
- Addressing cybersecurity vulnerabilities
- Providing training to operators
- Updating firmware and software

Integration Service Provider

The integration service provider is responsible for integrating new or upgraded IACS components into the existing infrastructure. This includes:

- Designing and deploying security solutions
- Configuring and managing security devices
- Testing and verifying security controls
- Documenting security procedures

Product Supplier

The product supplier is responsible for designing, developing, manufacturing, and supporting the IACS components. This includes:

- Integrating security into the product design
- Providing cybersecurity documentation
- Testing and validating security features
- Providing vulnerability management and security updates

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.

4 The ISA/IEC 62443 Series

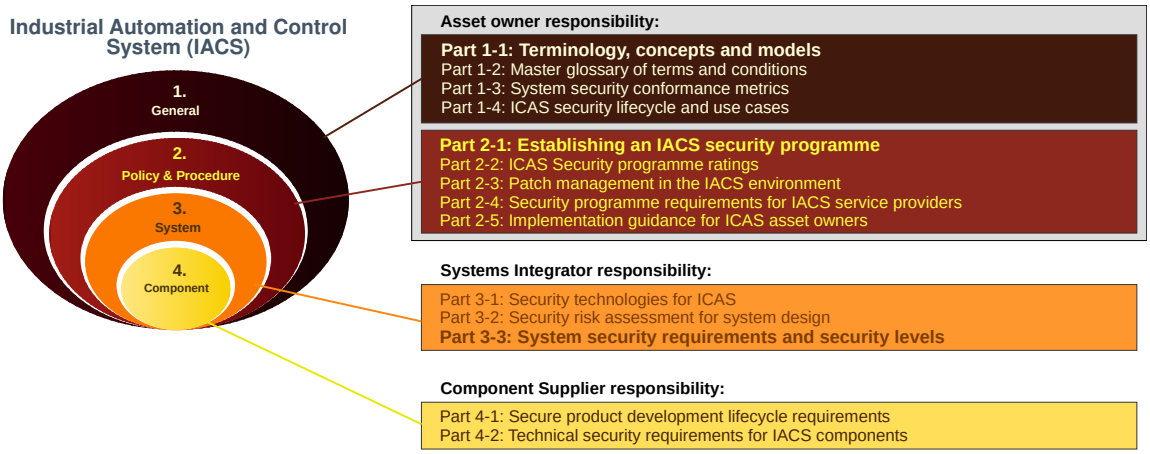


Figure 8: ISA/IEC 62443 Series

The ISA/IEC 62443 is a series of International Standards (IS), Technical Reports (TR) and Technical Specifications (TS) that together provide a flexible framework to address and mitigate security vulnerabilities in IACS. The documents are arranged in four groups as illustrated in Figure 8.

- **General**: Documents to address topics that are common across the entire series.
- **Policies and Procedures**: documents that focus on the policies and procedures associated with IACS security.
- **System Requirements**: documents that address requirements at the system level.
- **Component Requirements**: documents that provide information about the more specific and detailed requirements associated with the development of IACS products. These documents are the domain of system vendors who supply components of IACS systems.

5 ISA/IEC 62443 Part 1: General

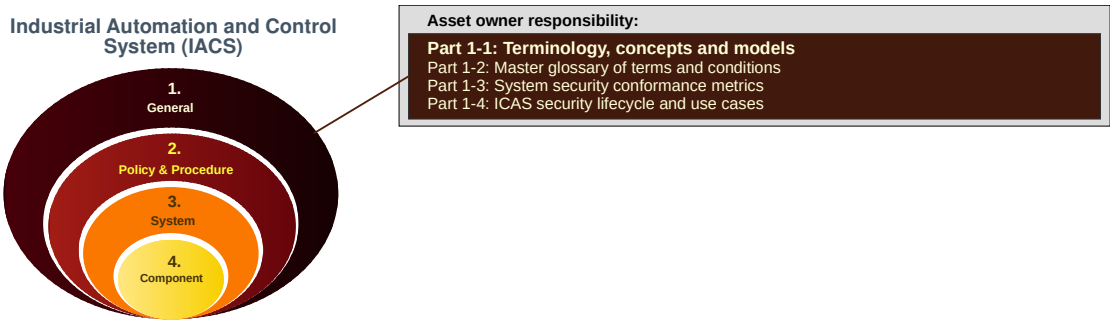


Figure 9: ISA/IEC 62443 Part 1: Overview and Vocabulary

The ISA/IEC 62443 Part 1: Overview and Vocabulary is a technical specification that provides a common language and framework for discussing IACS security. It defines the terminology and concepts used in the ISA/IEC 62443 series of standards and provides a general overview of IACS security.

5.1 ISA/IEC 62443-1-1: Terminology, Concepts, and Models

Part 1-1: Terminology, Concepts, and Models defines the common terminology and concepts used in the ISA/IEC 62443 series of standards for IACS security.

ISA/IEC 62443-1-1 standard defines over 300 terms related to IACS security. These terms are grouped into four categories:

- **Core concepts**: These terms are essential to understanding the ISA/IEC 62443 series of standards.
- **Security domains**: These terms are related to the different aspects of IACS security, such as asset security, communication security, and application security.
- **Security functions**: These terms are related to the specific security controls that can be implemented to protect IACS.
- **Security assurance**: These terms are related to the evaluation of the effectiveness of security controls.

5.1.1 Concepts

The ISA/IEC 62443-1-1 standard defines several important concepts related to IACS security, including:

- **Operational Technology**: The physical equipment and software that control industrial processes.
- **Information Technology**: The systems that manage and store digital information.
- **Cyber-physical systems (CPS)**: Systems that integrate IT and OT, making them more vulnerable to cyberattacks.
- **Attack surface**: The set of potential entry points that an attacker could use to compromise an IACS.

- **Vulnerability**: A weakness in a system that could be exploited by an attacker.
- **Risk**: The likelihood and severity of a negative event occurring.
- **Security posture**: The current state of security of an IACS.
- **Security programme**: A set of policies, procedures, and controls that are used to protect an IACS from cyberattacks.

5.1.2 Models

The ISA/IEC 62443-1-1 standard defines several models that can be used to represent IACS security, including:

- **Security zone model**: This model divides an IACS into security zones based on the criticality of the assets and the level of protection required.
- **Security architecture model**: This model defines the components of an IACS security architecture and their relationships.
- **Security risk management model**: This model provides a framework for identifying, analysing, and mitigating security risks.
- **Compliance model**: This model provides guidance on how to comply with relevant cybersecurity regulations.

5.2 Foundational Requirements

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 seven FRs. Each FR has several System Requirements (SR) as a part of system hardening against the foundation requirements. Each SR has a baseline requirement and zero or more a Requirement Enhancements (RE) within envelops of foundational system requirements to strengthen security.

5.2.1 FR 1 – Identification and Authentication Control (IAC)

Asset owner list of all users (humans, processes and devices) and to determine for each IACS component the required level of IAC protection.

- **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.

SR 1.1 User Identification and Authentication

- All human users shall be uniquely identified and authenticated.
- Users must be set up in the control system application.

SR 1.1 RE-2 Multi factor Authentication

- Multi-factor authentication for human users is required when accessing the system from/via untrusted networks.
- Compliance can be achieved by requiring Multi-factor Authentication when accessing the control network from/via an untrusted outside network, for instance by setting up VPN access to the network.

SR 1.2 Software process and device identification and authentication

- Identification and authentication of devices and software processes shall be implemented on interfaces providing access to the system.
- On Linux, user/group management.
- On Windows, user/group management in addition to allow listing processes in the Local Security Policy Editor and/or Windows Defender settings can be used.

SR 1.3 Account management

- The system must be able to manage all the users.
- User accounts can be managed in each OS through, for instance, Extensible Authentication Protocol (EAP), Kerberos, or Active Directory.
- Accounts on switches and other third-party equipment must also be handled.

SR 1.4 Identifier management

- Management of user, group, role, or control system interface identifiers must be supported.
- Linux and Windows have built-in support for this.
- Local policies and procedures must be established

SR 1.5 Authenticator management

- Must have procedures in place to make sure authenticators (such as passwords) are
- unique, not transmitted or stored in clear text, shared among employees, etc.
- An authenticator management system must be in place.

SR 1.6 Wireless access management

- It should be possible to identify and authenticate all users of Wireless communication.
- Ways to implement this is to require the devices to communicate using EAP methods, or by using Internet Protocol Security (IPSec) or Kerberos.
- In addition, allow listing of the communicating device addresses might add a barrier.

SR 1.7 Strength of password- based authentication

- When utilising password-based authentication, the strength of the password must be enforceable for the system, how to set minimum password length, variety of characters, lifetime, etc.
- Similar parameters are usually possible to enforce on the OS Level or through EAP.

SR 1.10 – Authenticator feedback

- The system shall not display the characters of a password when passwords are typed.
- Typically, an asterisk * is displayed instead of the typed password character.

SR 1.11 Unsuccessful login attempts

- It is possible to set up the maximum number of unsuccessful login attempts and lock-out time for the IACS.
- This can normally also be configured for user-accounts in the OS.

SR 1.12 System use notification

- System use notification messages that are displayed before authentication can be set up on the OS level in Linux and Microsoft Windows.
- Information that could be included in the message: Unauthorised use of the system is prohibited and subject to criminal and/or civil penalties.
- System usage is monitored, recorded, and subject to audit.
- Use of the system indicates consent to the above.
- It is not advisable to include too much information about the system being accessed, as this may assist the 'hacker' in applying a more system-specific attack.

SR 1.13 Access via untrusted networks

- The ability to monitor and control all methods of access from untrusted networks.
- Access to the IACS via untrusted networks should be restricted or protected.
- The number of security barriers to the system should be weighed against usability, with a focus on security.
- When possible, multi-factor authentication or some other strong security approach should be preferred.

SR 1.13 RE-1 Explicit access request approval

- Applicable control system operator(s) should have the ability to see that a remote session is ongoing, and it should be possible for an assigned role to terminate this remote-session.
- This means that a User Interface should have a way to show that a remote session is ongoing, and there should also be a way for the operator to sever that connection.
- Third-party hardware-based solutions exist that can help accommodate this requirement.

5.2.2 FR 2 – User Control (UC)

Asset owner assignment, to each user (human, process or device), the privileges defining the authorised use of the system. These are detailed in Security Requirements.

- **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.

SR 2.1 Authorisation enforcement

- Users and roles to be configured and the authorisation enforcement can be set as a complete system setting, down to a specific individual enforcement setting on an individual object (e.g. a parameter).
- The organisation must have procedures and practices in place to set this up correctly.

SR 2.2 Wireless use control

- The wireless network should be set up with the capability to authorise, monitor, and enforce usage restrictions according to commonly accepted security industry practices.
- Protocols such as EAP, Kerberos, or IPSec could be considered to improve handling this requirement.
- This requirement covers any means of wireless communication (Bluetooth, Zigbee, packet radio etc.).
- The IACS should be designed in such a way that usage of portable and mobile devices can be controlled.

SR 2.3 Use control for portable and mobile devices

- Context-specific authorisation should be required, and transfer of data using i.e USB should be restricted.

SR 2.4 Mobile code

- Software should not by default run any mobile code as part of the control system.
- The organisation must take care if files are retrieved from outside of the control system or exchanged within the control system network, that the files are fingerprinted and verified to prevent tampering.

SR 2.5 Session lock

- Session locks should not be used on systems where critical functions reside; Specifically, you should not have to 'log in' to perform an emergency shutdown of the IACS.
- When needed, session locks can typically be set up in the OS, so that the user is locked out and has to re-authenticate after a given timeout.

SR 2.6 Remote session termination

- It must be possible to set up remote sessions so that they terminate automatically after a specified inactivity- timeout, or using manual termination by the initiator.
- This can be configured in the OS or in a third party remote access solution.

SR 2.8 Auditable events

- The control system should be set up to produce auditable events into the system log.
- Prohibited access, changes to files and to the control system are amongst the events to record.
- A Security Information and Event Management (SIEM) system could be set up to handle the events from there.

SR 2.9 Audit storage capacity

- The Audit storage capacity should be large enough to accommodate the required logs.
- Mechanisms should be in place to prevent the capacity from being exceeded.

SR 2.10 Response to audit processing failures

- Failures in the audit processing system should alert operators and not cause loss of essential systems.
- There should be an alarm when disks are nearing full.

SR 2.11 Timestamps

- Timestamps should be used in all audit records.
- The control system can be configured to use an alternate time source as the OS clock or OS clocks in a distributed system may not be correct or synchronised.
- The time source used should be protected from unauthorised manipulation and tampering.
- GPS spoofing (and time manipulation) is a possibility that should be taken into account.

5.2.3 FR 3 – System Integrity (SI)

Asset owner must identify communication channels that require strong integrity protection.

- **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.

SR 3.1 Communication integrity

- Transmitted information should be protected.
- External solution such as IPSec can be set up to encapsulate the transmitted information.

SR 3.1 RE-1 Cryptographic integrity protection

- Transmitted information should be cryptographically protected, for instance using IPSec.
- This is typically used to prevent man-in-the-middle attacks where transmitted information is modified.
- This requirement is when communicating through/via untrusted networks.

SR 3.2 Malicious code protection

- Malicious code protection can be enforced by setting up Antivirus.
- The priority is set so that it does not interfere with the IACS real-time behaviour.
- An allow list of 'good' applications should be set up in the OS.

SR 3.2 RE-1 Malicious code protection on entry and exit points

- Malicious code protection can be enforced by setting up Antivirus.
- Disabling Autoplay and auto-mount can be seen as mitigating actions.

SR 3.3 Security functionality verification

- The solution must provide a way to (at least during test phases and scheduled maintenance) support safe verification of the security function.

SR 3.4 Software and information integrity

- The control system shall provide the capability to detect, record, report, and protect against unauthorised changes to software and information at rest.

SR 3.5 Input Validation

- The control system should validate any input used as a process input or any input that directly impacts the action of the control system.
- Set up input validation on all values that can be externally modified.
- Input is not only process data values. It can also be scripts, database queries, (potentially malformed) packets and other material that via tampering can change the working of the control-system.
- Set up reporting of anomalies to the SIEM system, as they may indicate system tampering and may assist in detecting a security breach.

SR 3.6 Deterministic Output

- It should be ensured that outputs go to a predefined state in the case when a normal operation can not be maintained as a result of an attack.
- This requires Input/Output (I/O) units and control applications to be set up so that they output the correct output when connection to the control system is lost, or when power is lost to (a part of) the system.
- This typically touches into the safe operation of a system; i.e. what is the 'safe' state of outputs.

SR 3.8 Session integrity

- Session-based protocols must be protected in a way that causes the rejection of invalid session Identifiers (ID).
- This can typically be done by adding a security layer such as IPSec or by using an encrypted transmission. Session-based protocols where this is not available should be avoided.

SR 3.8 RE-1 Invalidation of session IDs after session termination

- When session-based protocols are used, the session ID should be made invalid after use.
- When implementing your own session-based protocols, make sure that session IDs can not be reused after session termination.

SR 3.8 RE-2 Unique session ID generation

- Unique session IDs shall be created for each session.
- Sessions ID randomness must be ensured to prevent man-in-the-middle attacks and session hijacking.

SR 3.10 Support for updates

- Support for updates is required and this applies to each specific device type.
- The IACS must have a secure way to be updated and upgraded. By staying up-to-date, it is harder to exploit security weaknesses.
- The update process should be implemented in such a manner that it is not easily exploitable.

SR 3.14 Integrity of the boot process

- The IACS should be set up in such a way that it will verify the integrity of the firmware, software, and configuration data needed for the component’s boot and runtime processes before use.

5.2.4 FR 4 – Data Confidentiality (DC)

Some control system generated information whether at rest or in transit is of a confidential or sensitive nature.

- **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.

SR 4.1 Information confidentiality

- Confidential information should be secured in such a way that it is protected when it is at rest or in transit.
- Typical information could be users/passwords for managed devices, private keys, etc. Make sure to have procedures and processes in place to never expose confidential information.
- IEEE 802.1X port-based network access control could be used as a guard mechanism to gain access to the network.

SR 4.3 Use of cryptography

- When applicable, make sure to select 'industry standard' (or better) algorithms for cryptography.
- Wireless networks could use Wi-Fi Protected Access (WPA) version 3 (WPA3) (or better), and applicable I/O servers should be set up to use suitable (and 'industry approved') encryption standards.
- System backups and backups of keys etc. should also be protected using industry accepted cryptographic means.

5.2.5 FR 5 – Restricted Data Flow (RDF)

Asset owner must determine necessary information flow restrictions and determine the configuration of the conduits used to deliver this information.

- **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.

SR 5.1 Network segmentation

- Network segments should be logically isolated when possible.
- Routers or (managed) switches with virtual segmentation such as Virtual Local Area Network (VLAN) should be preferred and set up such that traffic from one segment does not intermix with traffic from other segments.
- If traffic from different segments is mixed, it is advisable to perform a Risk evaluation to see which barriers can be put in place to reduce the risk of a cyber incident.

SR 5.1 RE-1 Physical Network segmentation

- Network segments should be physically isolated so that control-system network and non-control system network traffic do not mix.

SR 5.2 Zone boundary protection

- Zone boundary protection should be enforced at zone boundaries.
- This can for instance be implemented using Remote Access Dial-In User Service (RADIUS), Trusted Network Connect, or some other Network Access Protocol.

SR 5.2 RE-1 Deny by default, allow by exception

- Network devices should be set up so that traffic is denied by default and allowed by exception.
- This, in addition to a scheme such as EAP, IPSec or Kerberos would add barriers that make it more difficult to hack the system.

SR 5.2 RE-2 Island mode

- The IACS should provide the capability to isolate itself from other networks to reduce the risk of being compromised when an attack is detected.

SR 5.3 General purpose person-to-person communication restrictions

- To mitigate an attack vector, the IACS should have the capability to prevent person-to-person messaging from and to the IACS.
- If such messaging is required, extensive compensating measures such as isolation and bandwidth-limiting should be employed to reduce the impact of an attack through this vector.

SR 5.4 Application partitioning

- Control applications should be partitioned based on criticality to implement a zoning model.
- Recommended using the modularity of the system to enforce this.
- Docker, or hypervisors, can segregate applications running on the same hardware, but make sure to assess any security and real-time performance implications this might have.

5.2.6 FR 6 – Timely Response to Events (TRE)

Asset owner must establish security policies and procedures and proper lines of communication and control needed to respond to security violations.

- **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.

SR 6.1 Audit log accessibility

- The audit logs should (only) be accessible for authorised users from a read-only device.
- There should be no way to modify the logs other than appending more log data from authorised sources.
- Access Control Lists (ACL), or 3rd party solutions might be a way to enforce this requirement.

5.2.7 FR 7 – Resource Availability (RA)

Asset owner must ensure that the system is resilient against various types of Denial-of-Service (DoS) attacks.

- **Rationale**: To ensure that the control system is resilient to various types of resource consuming attacks such as 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.

SR 7.1 DoS protection

- The IACS should have a way to request information from or be notified by boundary devices, or otherwise detect an ongoing cyberattack.
- Upon detection of a DoS attack, the IACS should operate in a degraded mode.
- A risk evaluation could be beneficial to see how to safely degrade the system in such a way that it does not adversely impact any safety-related systems.

SR 7.2 Resource management

- The IACS should be set up to provide resource management capabilities to mitigate resource exhaustion caused by security functions such as anti-virus checking and similar.
- The security functions should not cause the IACS to misbehave during operation.

SR 7.3 Control system backup

- The IACS should be set up so that up-to-date backups are available for full system recovery in the event of a system failure or misconfiguration.
- Audit logs and other forensic information should be included in the backup(s).
- To protect confidential information, backups could be encrypted.
- It is important to note that the control system should be in a safe state when doing a backup.

SR 7.4 Control system recovery and reconstitution

- There should be a way to quickly and safely recover the control system to a known secure state after a failure or disruption has occurred.
- For industrial controllers, this typically means restoring the latest backup.
- Other stateful devices such as managed switches and I/O units must also have the capability to be restored to a matching last known secure state.
- This typically means that firmware and settings must be available to restore, or that a verified spare part with the correct configuration is available to swap out the defective unit.

SR 7.5 Emergency power

- The IACS should be able to switch to and from the emergency power supply without affecting the existing security state or a documented degraded mode.
- It might be wise to do a Risk assessment to determine probable causes of failures and to implement barriers to mitigate these.

SR 7.6 Network and security configuration settings

- The solution shall provide guidelines for network and security configurations, and the IACS shall be able to be configured accordingly.
- The OS should be configured according to the OS guidelines, and the IACS should be set up to monitor and control changes to these configuration settings in accordance with security policies and procedures.

SR 7.7 Least functionality

- The IACS should restrict the use of unnecessary functions.
- It is advised to set up firewalls to only allow the known device addresses, services, and ports to be used.
- On Linux, this can be done by using iptables/nftables and on Windows this can be done by utilising for instance the Windows Firewall.

5.3 ISA/IEC 62443-1-2: 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.

5.4 ISA/IEC 62443-1-3: System Security Conformance Metrics

The Part 1-3 technical specification defines the requirements for developing quantitative metrics to measure the conformance of IACS systems to the ISA/IEC 62443 family of standards. This provides a framework for organisations to measure and evaluate the security posture of their IACS systems. This is important because it helps organisations to identify and address security vulnerabilities and weaknesses. By using the metrics defined in the standard, organisations can also demonstrate their compliance with the ISA/IEC 62443 family of standards.

The standard defines a set of high-priority metrics that focus on security technical control functions. These metrics are derived from the FRs, SRs, and other guidance material in the ISA/IEC 62443 standards.

The standard also defines a methodology for developing additional metrics to address specific security requirements or to measure the conformance of specific IACS components.

5.4.1 Metrics and Measurements

The metrics are grouped into the following categories:

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

Each metric is defined in a way that makes it measurable and quantifiable. For example, the asset security metric for asset identification might be the number of assets that have been uniquely identified and classified.

5.4.2 Measurement Approach

The standard also defines a methodology for measuring the conformance of IACS systems to the metrics. This methodology includes the following steps:

- **Data collection**: The first step is to collect data about the IACS system. This data can be collected from a variety of sources, such as network traffic logs, vulnerability scans, and security configuration management systems.
- **Data analysis**: The next step is to analyse the data to identify any deviations from the metrics. This analysis can be performed manually or using automated tools.
- **Action planning**: Once the deviations have been identified, the organisation should develop a plan to address them. This plan should include the specific actions that will be taken to remediate the deviations and the time-frame for completing the remediation.
- **Monitoring and improvement**: The organisation should continue to monitor the IACS system and the metrics to ensure that the conformance is maintained. The organisation should also regularly review and update the action plan as needed.

5.5 ISA/IEC 62443-1-4: IACS Security Lifecycle and Use Cases

Part 1-4 is a technical specification that defines a framework for implementing IACS security throughout the lifecycle of an IACS.

5.5.1 Lifecycle Stages

The ISA/IEC 62443-1-4 standard defines four stages of the IACS security lifecycle:

- **Design**: This stage involves defining the security requirements for the IACS and developing security controls to meet those requirements.
- **Implementation**: This stage involves implementing the security controls that were defined in the design stage.
- **Operation**: This stage involves operating and maintaining the IACS in a secure manner.
- **Retirement**: This stage involves decommissioning the IACS and disposing of it in a secure manner.

5.5.2 Use Cases

The standard defines a set of use cases that illustrate how the standard can be applied to different types of IACS and different types of security requirements. The use cases cover a wide range of scenarios, including:

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

5.5.3 Key Requirements

The standard reaffirms the core principles for implementing IACS security throughout the lifecycle. These requirements are divided into four main categories:

- **Security by design**: IACS security should be considered from the earliest stages of system development and should be integrated into the overall design and architecture.
- **Security by default**: Default configurations should be secure and should not require additional configuration to be secure.
- **Security throughout the lifecycle**: Security should be maintained throughout the entire lifecycle of the IACS, from design and development to operation and maintenance.
- **Security risk management**: Security should be based on a risk-management approach that considers the specific threats, vulnerabilities, and consequences of a security breach.

6 Laboratory #1 – ISA/IEC 62443 Risk Assessment

Your lecturer will work through this laboratory with you during class.

7 Bibliography

[1] ISA/IEC 62443, ‘Industrial communication networks - IT security for networks and systems’. International Society of Automation/International Electrotechnical Commission, Jul. 20, 2009.
[2] NIST, ‘Cybersecurity Framework 2.0’, National Institute of Standards and Technology, Aug. 2023. Accessed: Aug. 22, 2023. [Online]. Available: https://doi.org/10.6028/NIST.CSWP.29.ipd
[3] G. Blokdyk, *NERC CIP a Complete Guide - 2020 Edition*. Emereo Pty Limited, 2019. [Online]. Available: https://books.google.ie/books?id=ZBCyywEACAAJ

This page is intentionally blank