ISA/IEC 62443 Quick Reference

ISA/IEC 62443 is a Cybersecurity standard offering guidance on Automation and Control Systems (ACS). Note that ISA 62443 and IEC 62443 are substantially identical. As of January 2025, titles and descriptions are as follows. However, these may change over time, so to be certain, refer to the latest version from ISA or IEC.

- **62443-1-1: Terminology, concepts and models**
  Introduces the concepts and models used throughout the series.

- **62443-1-5: Scheme for IEC 62443 security profiles**
  Specifies a scheme for defining (selecting, writing, drafting, and creating) IEC 62443 security profiles.

- **62443-2-1: Security program requirements for asset owners**
  Defines the requirements and provides guidance to develop an automation and control system security program for asset owners.

- **62443-2-3: Patch management in the ACS environment**
  Describes a format for the exchange of information about the status of patches and their applicability and provides guidance on planning and building a patch management program within asset owner, service provider, and product supplier organizations.

- **62443-2-4: Security program requirements for ACS service providers**
  Contains security requirements for providers of integration service including commissioning activities, and maintenance service for ACS.

- **62443-3-1: Security Technologies for Industrial automation and control systems**
  Surveys and provides an evaluation and assessment of many current types of electronic- based cyber security technologies that may apply to protecting an ACS environment from detrimental cyber intrusions and attacks.

- **62443-3-2: Security risk assessment for system design**
  Describes the activities required to perform security risk assessments on a new or existing ACS and the design activities required to mitigate the risk to tolerable levels.

- **62443-3-3: System security requirements and security levels**
  Describes the technical security requirements for systems related to the seven foundational requirements defined in ISA 62443-1-1 and assigns system security levels (SLs) to the equipment under control.

- **62443-4-1: Secure product development lifecycle requirements**
  Describes product development lifecycle requirements related to cyber security for products (i.e., components and systems) intended for use in the ACS and provides guidance on how to meet the requirements described for each element.

- **62443-4-2: Technical security requirements for ACS components**
  Describes the technical security requirements for the components that are used to build automation and control systems. These requirements are derived from the system requirements for ACS defined in ISA 62443-3-3, and as such, assigns component SLs based on the system security levels

- **62443-6-1: Security evaluation methodology for IEC 62443-2-4**
  Specifies the evaluation methodology to support interested parties (e.g. during conformity assessment activities) to achieve repeatable and reproducible evaluation results against IEC 62443-2-4 requirements.

- **62443-6-2: Security evaluation methodology for IEC 62443-4-2**
  Specifies the evaluation methodology to support interested parties (e.g. during conformity assessment activities) to achieve repeatable and reproducible evaluation results against IEC 62443 - 4-2 requirements.

Security Levels

The ISA 62443 series specifies four different security levels (1, 2, 3, and 4), each with an increasing level of security. They apply to technical, physical, and process security measures, including how these security measures are implemented during the operation of the ACS.

Types of Security Levels

Security Levels may be expressed as different types depending on their purpose and use within the security lifecycle.
Types of Security Levels defined in the ISA 62443 standards are:

- **Capability security levels (SL-C)** are the security levels that components or systems can provide when properly configured. These levels state that a particular component or system is capable of meeting the target SLs natively without additional compensating security measures when properly configured and integrated.

- **Target security levels (SL-T)** are the desired level of security for a particular system. This is usually determined by performing a risk assessment on a system and determining that it needs a particular level of security to ensure its correct operation.

- **Implemented security levels (SL-I)** are the actual level of security for a particular system. These are measured after a system design is available or when a system is in place. They are used to establish that a security system is meeting the goals that were originally set out in the target security levels.

- **Operational security levels (SL-O)** is the actual security level provided during the operation of an ACS. They describe the security level when all technical, physical and process security measures are in place and is determined during the operation and maintenance phases of the ACS.

Maturity Levels

ACS Owner measures conformance with security requirements through 4 maturity levels.

ML 1: Initial: Processes are performed in an ad-hoc or undocumented manner
ML 2: Managed: Processes are documented and describe how to manage the delivery and performance of the activity
ML 3: Defined/Practiced: Processes are documented, executed, and repeatable
ML 4: Improving: Processes are improved over time using metrics for performance and effectiveness

ISA/IEC 62443 Quick Reference

Foundational Requirements (FR1 to FR7)

1. Identification, authentication & access control (FR1)	5. Restrict data flow (FR5)
2. Use control (FR2)	6. Timely response to event (FR6)
3. System integrity (FR3)	7. Resource availability (FR7)
4. Data confidentiality (FR4)	

ISA/IEC 62443-2-1:2024 Provides:

- Security program requirements for ACS asset owner including mapping between:
  - Security Program Elements (SPE) in 62443-2-1,
  - System security requirements in ISA/IEC 62443-3-3, and
  - Component security requirements in ISA/IEC 62443-4-2.
  - How to integrate shared responsibilities between different Principal Roles who deal with ACS.

ISA/IEC 62443-2-1:2024 "Security Program requirements for IACS asset owner"

Security Program Element	Requirements	Security Control		ML1 Initial	ML2 Managed	ML3 Defined (Practiced)	ML4 Improving
SPE 1 – Organizational security measures	ORG 1 – Security related organization and policies	ORG 1.1	Information security management system (ISMS).				
		ORG 1.2	Background checks				
		ORG 1.3	Security roles and responsibilities				
		ORG 1.4	Security awareness training				
		ORG 1.5	Security responsibilities training				
		ORG 1.6	Supply chain security				
	ORG 2 – Security assessments and reviews	ORG 2.1	Security risk mitigation				
		ORG 2.2	Processes for discovery of security anomalies				
		ORG 2.3	Secure development and support				
		ORG 2.4	SP reviews				
	ORG 3 – Security of physical access	ORG 3.1	Physical access control				
SPE 2 – Configuration management	CM 1 – Inventory management of IACS hardware/software components and network communications .	CM 1.1	Asset inventory baseline				
		CM 1.2	Infrastructure drawings/documentation				
		CM 1.3	Configuration settings				
		CM 1.4	Change control				
SPE 3 – Network and communications security	NET 1 – System segmentation	NET 1.1	Segmentation from non-IACS zones				
		NET 1.2	Documentation of zones and network zone interconnections				
		NET 1.3	Network segmentation from safety systems				
		NET 1.4	Network autonomy				
		NET 1.5	Network disconnection from external networks .				
		NET 1.6	Internal network access control				
		NET 1.7	Network accessible services				
		NET 1.8	User messaging				
		NET 1.9	Network time distribution				
	NET 2 – Secure wireless access	NET 2.1	Wireless protocols				
		NET 2.2	Wireless network segmentation				
		NET 2.3	Wireless properties and addresses				
	NET 3 – Secure remote access	NET 3.1	Remote access applications				
		NET 3.2	Remote access connections				
		NET 3.3	Remote access termination				
SPE 4 – Component security	COMP 1 – Components and portable media	COMP 1.1	Component hardening				
		COMP 1.2	Dedicated portable media				
	COMP 2 – Malware protection	COMP 2.1	Malware free				
		COMP 2.2	Malware protection				
		COMP 2.3	Malware protection software validation and installation				
	COMP 3 – Patch management	COMP 3.1	Security patch authenticity/integrity				
		COMP 3.2	Security patch validation and installation				
		COMP 3.3	Security patch status				
		COMP 3.4	Security patching retention of security				
		COMP 3.5	Security patch mitigation				
SPE 5 – Protection of data	DATA 1 – Protection of data	DATA 1.1	Data classification				
		DATA 1.2	Data confidentiality				
		DATA 1.3	Safety system configuration mode				
		DATA 1.4	Data retention policy				
		DATA 1.5	Cryptographic mechanisms				
		DATA 1.6	Key management				
		DATA 1.7	Data Integrity				
SPE 6 – User access control	USER 1 – Identification and authentication	USER 1.1	User identity assignment				
		USER 1.2	User identity removal				
		USER 1.3	User identity persistence				
		USER 1.4	Access rights assignment				
		USER 1.5	Least privilege				
		USER 1.6	Software service authentication				
		USER 1.7	Software services interactive login rights				
		USER 1.8	Human user authentication				
		USER 1.9	Multifactor authentication (MFA)				
		USER 1.10	Mutual authentication				
		USER 1.11	Password protection				
		USER 1.12	Shared and disclosed/compromised passwords				
		USER 1.13	User login display information				
		USER 1.14	User login failure displays				
		USER 1.15	Consecutive login failures				
		USER 1.16	Session integrity				
		USER 1.17	Concurrent sessions				
		USER 1.18	Screen Lock				
		USER 1.19	Component authentication				
	USER 2 – Authorization and access control	USER 2.1	Authorization				
		USER 2.2	Separation of duties				
		USER 2.3	Multiple approvals				
		USER 2.4	Manual elevation of privileges				
SPE 7 – Event and incident management	EVENT 1 – Event and incident management	EVENT 1.1	Event detection				
		EVENT 1.2	Event reporting				
		EVENT 1.3	Event reporting interfaces				
		EVENT 1.4	Logging				
		EVENT 1.5	Log entries				
		EVENT 1.6	Log access				
		EVENT 1.7	Event analysis				
		EVENT 1.8	Incident handling and response				
		EVENT 1.9	Vulnerability handling				
SPE 8 – System integrity and availability	AVAIL 1 – System availability and intended functionalit	AVAIL 1.1	Continuity management				
		AVAIL 1.2	Resource availability management				
		AVAIL 1.3	Failure-state				
	AVAIL 2 – Backup/restore/archive	AVAIL 2.1	Backup				
		AVAIL 2.2	Backup non-interference				
		AVAIL 2.3	Backup verification				
		AVAIL 2.4	Backup media				
		AVAIL 2.5	Backup restoration				