ISA/IEC 62443 Quick Reference

ISA/IEC 62443 is a Cybersecurity standard offering guidance on Automation and Control Systems (ACS). Note that these document titles and descriptions may change, so check 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.

ISA/IEC 62443 Quick Reference

Security Levels

The ISA 62443 series specify four different security levels (1, 2, 3, and 4), each with an increasing level of security. These measures pertain to technical, physical, and process security aspects, including their implementation during ACS operations.

Types of Security Level

Security Levels may be expressed as different types depending on their purpose and use within the security lifecycle. Types of Security Level 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
ML 3: Defined/Practiced: Processes are documented, executed, and repeatable
ML 4: Improving: Processes are improved over time using metrics for performance and effectiveness

Foundational Requirements (FR1 to FR7)

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