# Introduction to IEC 62443

## The International Standard for Industrial Cyber-security

OT Security Learning Series

Document 110 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance



LEARNING RESOURCE

# Contents

# 1 What is IEC 62443?

**IEC 62443** is the international standard series for cybersecurity in Industrial Automation and Control Systems (IACS). Developed by the International Electrotechnical Commission (IEC) in collaboration with ISA (International Society of Automation), it provides a comprehensive framework for securing industrial systems.

**Information**

IEC 62443 is often referred to as **ISA/IEC 62443** because it originated from the ISA99 committee's work. The standards are technically equivalent – ISA-62443 and IEC 62443 can be used interchangeably.

## 1.1 Why IEC 62443?

Traditional IT security standards (like ISO 27001) don't fully address the unique requirements of OT environments:

- **Availability over Confidentiality:** In OT, system uptime is critical
- **Safety Requirements:** Industrial systems can cause physical harm
- **Legacy Systems:** 20+ year old equipment can't be easily patched
- **Real-time Constraints:** Security can't introduce latency
- **Different Lifecycles:** OT systems run for decades, not years

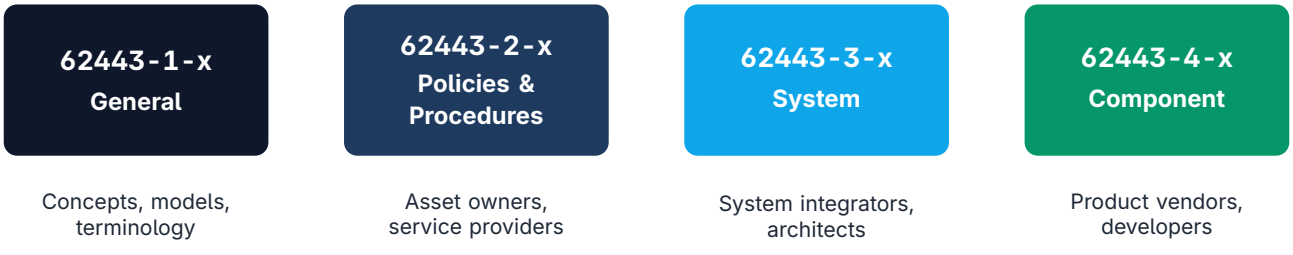
**Key Point**

IEC 62443 provides a **risk-based approach** that balances security requirements with operational needs, covering the entire lifecycle from design to decommissioning.

# 2 Standard Structure

IEC 62443 is organized into four main series, each addressing different stakeholders and aspects of industrial cybersecurity.

## 2.1 The Four Series



## 2.2 Key Documents

**Most Referenced Standards**

| | |
|---|---|
| **62443-1-1** | Terminology, concepts, and models |
| **62443-2-1** | Security program requirements for asset owners |
| **62443-2-4** | Security program requirements for service providers |
| **62443-3-2** | Security risk assessment and zone/conduit design |
| **62443-3-3** | System security requirements and security levels |
| **62443-4-1** | Secure product development lifecycle |
| **62443-4-2** | Technical security requirements for components |

# 3 Security Levels (SL)

One of the most important concepts in IEC 62443 is the **Security Level** (SL). Security levels define the degree of protection required against different threat actors.

## 3.1 The Four Security Levels

**SL 1 Security Level 1 – Casual/Coincidental**

**Threat Actor:** Unintentional errors, accidental exposure
**Protection Against:**
- Accidental or unintentional violations
- Casual exploration by curious individuals
- Basic automated tools and scripts

**Example:** Employee accidentally clicking a phishing link

**SL 2 Security Level 2 – Intentional/Simple Means**

**Threat Actor:** Low motivation, limited resources, general skills
**Protection Against:**
- Intentional attacks using simple techniques
- Low-resource hackers and script kiddies
- Common malware and known exploits

**Example:** Opportunistic attacker using publicly available tools

**SL 3 Security Level 3 – Intentional/Sophisticated Means**

**Threat Actor:** Moderate motivation, sophisticated tools, IACS-specific skills
**Protection Against:**
- Sophisticated attacks with IACS knowledge
- Organized crime groups
- Targeted attacks on specific organizations

**Example:** Targeted ransomware attack on industrial facility

**SL 4 Security Level 4 – Intentional/State-Sponsored**

**Threat Actor:** High motivation, extended resources, nation-state capabilities
**Protection Against:**
- Nation-state actors and APT groups
- Extended campaigns with significant resources
- Zero-day exploits and custom malware

**Example:** Stuxnet-style targeted attack on critical infrastructure

### 3.2 Security Level Types

IEC 62443 defines three types of security levels:

| Type | Description |
|---|---|
| **SL-T** (Target) | The desired security level based on risk assessment |
| **SL-A** (Achieved) | The actual security level measured/tested |
| **SL-C** (Capability) | The maximum level a component/system can achieve |

**Warning**

The goal is to ensure: **SL-A** $\geq$ **SL-T**
If your achieved security level is lower than your target, you have a security gap that must be addressed through compensating controls or system upgrades.

## 4 Zones and Conduits

IEC 62443 uses the concept of **zones** and **conduits** for network segmentation and risk management.

## 4.1 Zones

**Zone Definition**

A **zone** is a logical or physical grouping of assets that share common security requirements based on:

- Criticality and consequence of compromise
- Required security level
- Physical or logical location
- Responsible organization

Each zone has a single **target security level** (SL-T). Assets within a zone should have similar security requirements.

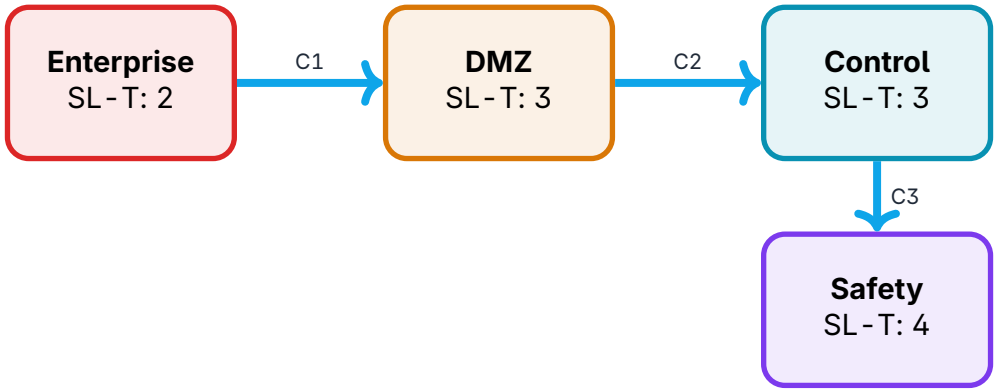
## 4.2 Conduits

**Conduit Definition**

A **conduit** is a logical grouping of communication channels that share common security requirements and connect two or more zones.

Conduits must provide security controls appropriate to protect both connected zones. The conduit's security level should match or exceed the highest SL-T of the connected zones.

## 4.3 Zone and Conduit Diagram




# 5 Foundational Requirements (FR)

IEC 62443-3-3 defines seven **Foundational Requirements** (FRs) that form the basis of all security controls.

| FR | Name | Description |
|---|---|---|
| **FR 1** | Identification & Authentication | Control who and what can access the system |
| **FR 2** | Use Control | Control what authenticated users can do |
| **FR 3** | System Integrity | Ensure the system operates correctly |
| **FR 4** | Data Confidentiality | Protect sensitive data from disclosure |
| **FR 5** | Restricted Data Flow | Segment networks and control data flow |
| **FR 6** | Timely Response | Respond to security violations |
| **FR 7** | Resource Availability | Ensure system availability against DoS |

Each FR contains multiple **System Requirements** (SRs) and **Requirement Enhancements** (REs) that specify detailed controls for each security level.

**Tip**

When implementing IEC 62443, start with the FRs and map them to your existing controls. This gap analysis helps prioritize security improvements.

# 6 Roles and Responsibilities

IEC 62443 defines clear responsibilities for different stakeholders:

## 6.1 Asset Owner

- Defines security requirements (SL-T) based on risk assessment
- Implements and maintains security program (62443-2-1)
- Responsible for overall OT security governance
- Verifies that SL-A meets SL-T

## 6.2 System Integrator

- Designs systems to meet SL-T requirements
- Implements zones, conduits, and security controls
- Follows secure integration practices (62443-2-4)
- Documents achieved security level (SL-A)

## 6.3 Product Vendor

- Develops products following secure lifecycle (62443-4-1)
- Documents product security capabilities (SL-C)
- Provides security patches and updates

- Certifies products against 62443-4-2

## 7 Certification

IEC 62443 certification is offered by several organizations including TUV, Exida, and ISASecure.

### 7.1 Certification Types

- **Component Certification** (62443-4-2): Individual products
- **SDLC Certification** (62443-4-1): Development processes
- **System Certification** (62443-3-3): Complete systems
- **Capability Certification**: Organization processes

**Information**

Certification provides independent verification of security claims but is not mandatory. Many organizations use IEC 62443 as a framework without formal certification.

## 8 Summary

**Key Takeaways**

| | |
|---|---|
| **IEC 62443** | Comprehensive standard for industrial cybersecurity |
| **Security Levels** | SL 1-4 define protection against threat actors |
| **Zones/Conduits** | Network segmentation methodology |
| **7 FRs** | Foundational requirements covering all security aspects |
| **Stakeholders** | Asset owners, integrators, and vendors have defined roles |

**Key Point**

IEC 62443 provides a **common language** for discussing OT security requirements between asset owners, integrators, and vendors. Even partial adoption improves security posture.

## 9 Next Steps

To start implementing IEC 62443 in your organization:

1. **Inventory:** Document all IACS assets and their criticality
2. **Risk Assessment:** Determine SL-T for each zone (62443-3-2)

3. **Gap Analysis:** Compare current state (SL-A) to target (SL-T)
4. **Roadmap:** Prioritize improvements based on risk
5. **Procurement:** Require 62443-4-2 compliance for new products

## 10 Further Reading

### Standards

- **ISA/IEC 62443 Series** – Complete Standards Collection
  https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
- **IEC 62443-2-1** – Security Program Requirements for Asset Owners
- **IEC 62443-3-3** – System Security Requirements and Security Levels
- **IEC 62443-4-2** – Technical Security Requirements for IACS Components

### Resources

- **NIST SP 800-82 Rev. 3** – Guide to OT Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final
- **CISA ICS-CERT** – Industrial Control Systems Advisories
  https://www.cisa.gov/news-events/ics-advisories
- **ISASecure** – IEC 62443 Certification Information
  https://isasecure.org/

### Books

- Knapp, E. & Langill, J. – *Industrial Network Security* (Syngress)
- Macaulay, T. & Singer, B. – *Cybersecurity for Industrial Control Systems* (CRC Press)