IEC 62443 Security Levels

Mapping security solutions to SL1–SL4 requirements

OT Security Learning Series

Document 120 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

IEC 62443 defines four Security Levels (SL1–SL4) that represent increasing levels of protection against different threat actors. This document maps practical security solutions to each level.

1.1 Security Level Definitions

SL	Threat Actor	Description
SL 1	Casual/Accidental	Protection against unintentional errors
SL 2	Intentional, Low Resources	Script kiddies, disgruntled employees
SL 3	Intentional, Moderate Resources	Hacktivists, organized crime
SL 4	Intentional, High Resources	Nation-states, APT groups

Table 1: IEC 62443 Security Levels

Warning

Most industrial environments should target **SL2** as a baseline. Critical infrastructure (energy, water, chemical) typically requires **SL3**. **SL4** is reserved for high-value national security targets.

2 Foundational Requirements Overview

IEC 62443-3-3 defines seven Foundational Requirements (FR):

FR	Name	Focus Area
FR1	Identification & Authentication	User and device identity
FR2	Use Control	Authorization and privileges
FR3	System Integrity	Protection from tampering
FR4	Data Confidentiality	Protection of sensitive data
FR5	Restricted Data Flow	Network segmentation
FR6	Timely Response to Events	Monitoring and incident response
FR7	Resource Availability	Denial of service protection

Table 2: IEC 62443 Foundational Requirements

3 FR1: Identification & Authentication

FR1 – Identification & Authentication

Controls for identifying and authenticating users, processes, and devices before granting access to system resources.

Level	Security Solutions
SL 1	› Unique user accounts (no shared accounts) › Basic password policy (8+ characters) › Device identification by IP/hostname
SL 2	› Strong password policy (complexity, expiration) › Role-based access control (RBAC) › Central authentication (Active Directory) › Device certificates for critical systems
SL 3	› Multi-factor authentication (MFA) › Hardware tokens or smart cards › Certificate-based device authentication › Privileged Access Management (PAM)
SL 4	› Biometric authentication › Hardware Security Modules (HSM) › Mutual TLS for all connections › Continuous authentication/verification

Table 3: FR1 Solutions by Security Level

4 FR2: Use Control

FR2 – Use Control

Controls for enforcing assigned privileges to ensure only authorized actions are performed.

Level	Security Solutions
SL 1	› Basic user permissions on HMI/workstations › Separate operator vs. engineer accounts › Session timeout after inactivity
SL 2	› Granular role-based access control › Principle of least privilege enforced › Automatic session lock › Audit logging of privilege use
SL 3	› Attribute-based access control (ABAC) › Just-in-time (JIT) privilege elevation › Dual authorization for critical actions › Comprehensive access reviews
SL 4	› Four-eyes principle for all changes › Real-time privilege monitoring › Automated policy enforcement › Zero-trust access model

Table 4: FR2 Solutions by Security Level

5 FR3: System Integrity

FR3 – System Integrity

Controls to ensure systems and data are protected from unauthorized changes.

Level	Security Solutions
SL 1	› Antivirus on Windows systems › Basic change management process › Manual configuration backups
SL 2	› Application whitelisting › File integrity monitoring (FIM) › Automated backup and verification › Patch management process
SL 3	› Code signing for all executables › PLC program integrity verification › Secure boot / trusted boot › Configuration management database
SL 4	› Hardware root of trust (TPM) › Cryptographic integrity verification › Automated drift detection and remediation › Air-gapped golden image repository

Table 5: FR3 Solutions by Security Level

6 FR4: Data Confidentiality

FR4 – Data Confidentiality

Controls to protect data from unauthorized disclosure.

Level	Security Solutions
SL 1	› Password-protected engineering files › Physical access control to servers › Basic network separation
SL 2	› Encrypted remote access (VPN) › HTTPS for web interfaces › Encrypted database storage › Data classification policy
SL 3	› End-to-end encryption (OPC UA Secure) › Full disk encryption › DLP (Data Loss Prevention) › Encrypted protocol tunnels
SL 4	› Hardware encryption (self-encrypting drives) › Encrypted memory › Quantum-resistant cryptography planning › Data diodes for sensitive flows

Table 6: FR4 Solutions by Security Level

7 FR5: Restricted Data Flow

FR5 – Restricted Data Flow

Controls for network segmentation and data flow enforcement between zones.

Level	Security Solutions
SL 1	› Basic firewall between IT and OT › VLAN separation › Default deny rules
SL 2	› Industrial DMZ architecture › Stateful firewall inspection › Jump servers for remote access › Network access control (NAC)
SL 3	› Deep packet inspection (DPI) for OT protocols › Micro-segmentation within OT › Application-aware firewalls › Unidirectional gateways (data diodes)
SL 4	› Hardware-enforced data diodes › Air-gapped safety systems › Protocol break/proxy for all flows › Zero-trust network architecture

Table 7: FR5 Solutions by Security Level

8 FR6: Timely Response to Events

FR6 – Timely Response to Events

Controls for monitoring, logging, and responding to security events.

Level	Security Solutions
SL 1	› Local logging on critical systems › Basic alerting for system failures › Manual log review process
SL 2	› Centralized log collection (SIEM) › OT network monitoring / IDS › Documented incident response plan › Regular IR drills
SL 3	› OT-specific anomaly detection › 24/7 Security Operations Center › Automated threat intelligence feeds › Forensic readiness procedures
SL 4	› AI/ML-based threat detection › Automated response playbooks (SOAR) › Dedicated OT SOC › Real-time threat hunting

Table 8: FR6 Solutions by Security Level

9 FR7: Resource Availability

FR7 – Resource Availability

Controls to ensure systems remain available under adverse conditions.

Level	Security Solutions
SL 1	› UPS for critical systems › Regular backups › Basic spare parts inventory
SL 2	› Redundant network paths › Hot standby for critical servers › DoS protection on perimeter › Tested recovery procedures
SL 3	› Redundant controllers (1oo2, 2oo3) › Geographic redundancy for critical data › Rate limiting on all interfaces › Automated failover testing
SL 4	› Full system redundancy › Isolated backup control room › Electromagnetic pulse (EMP) protection › Continuous availability validation

Table 9: FR7 Solutions by Security Level

10 Implementation Guidance

Key Point

Start with an SL assessment to determine your target level, then use this mapping to select appropriate security solutions. Not every control is needed—focus on your specific risks and asset criticality.

10.1 Assessment Approach

1. **Identify zones and conduits** – Map your OT architecture
2. **Determine target SL** – Based on risk assessment and threat analysis
3. **Gap analysis** – Compare current state to target SL requirements
4. **Prioritize** – Address highest-risk gaps first
5. **Implement incrementally** – Don't try to reach SL3 overnight

10.2 Common Pitfalls

- Applying IT solutions without OT adaptation
- Targeting SL4 when SL2 is sufficient
- Ignoring operational impact of security controls

- Focusing on technology without processes and training

11 Summary

Key Takeaways

- **SL1–SL4** – Increasing protection against sophisticated threats
- **7 Foundational Requirements** – Comprehensive security coverage
- **SL2 baseline** – Appropriate for most industrial environments
- **SL3 for critical infrastructure** – Energy, water, chemical sectors
- **Incremental approach** – Build security maturity over time
- **Balance security and operations** – OT availability is paramount

12 Further Reading

Standards

- **IEC 62443-3-3** – System security requirements and security levels
  https://webstore.iec.ch/publication/7033
- **IEC 62443-2-1** – Security program requirements for asset owners
  https://webstore.iec.ch/publication/7030

Resources

- **ISA/IEC 62443 Series Overview**
  https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
- **CISA – ICS Security**
  https://www.cisa.gov/topics/industrial-control-systems

Part of the OT Security Learning Series