

IEC 62443-4-2:2019

IEC 62443-4-2 specifies technical security requirements for industrial automation and control system components to protect them from cyber threats.



What it is

IEC 62443-4-2 is an international cybersecurity standard that establishes technical security requirements for components of industrial automation and control systems (IACS). The framework aims to help organizations secure devices such as industrial controllers, network components, and software applications against evolving cyber threats.

Developed and published by the International Electrotechnical Commission (IEC), IEC 62443-4-2 is used by manufacturers, system integrators, and asset owners in industries like energy, manufacturing, and critical infrastructure. The standard outlines detailed security controls and requirements addressing areas such as authentication, access control, data integrity, confidentiality, and secure communications within IACS environments.

At a glance

PUBLISHER International Electrotechnical Commission (IEC)	TYPE Framework	VERSION 2019
EFFECTIVE 2019	DOMAIN Cybersecurity	FAMILY ISO Industry Standards
REGION International	INDUSTRY Critical Infrastructure	ADOPTION MODEL Industry Requirement
IMPLEMENTATION COMPLEXITY Very High		

Source: <https://webstore.iec.ch/publication/34421>

Why it matters

- **Strengthen OT security governance** Establish clear security requirements for industrial components that support effective oversight of operational technology cybersecurity.
- **Enhance regulatory compliance** Support alignment with industrial cybersecurity standards and regulations through component-level security requirements mapped to international standards.
- **Reduce attack surface** Implement component-level security controls that minimize vulnerabilities in industrial automation and control systems.
- **Support operational resilience** Ensure industrial components meet security requirements that reduce the risk of cyber incidents affecting critical operations.

How SmartSuite supports IEC 62443-4-2

Component Security Requirements Library Structure technical requirements for IACS components with clear ownership.	Verification and Test Evidence Track security verification activities and store test results tied to requirements.	Secure Configuration and Hardening Document secure defaults, hardening guidance, and controlled configuration changes.
Vulnerability Management Workflow Manage findings, remediation plans, retesting, and release approvals.	Supplier and Remote Access Oversight Track vendor access, maintenance procedures, and supporting evidence for compliance.	Assessment and Audit Reporting Provide a clear view of requirement status, exceptions, and open remediation.

Common framework mappings

Official resources

IEC 62443-4-2 Standard
Defines technical security requirements for components of industrial automation and control systems.
webstore.iec.ch/publication/34421

Frequently asked questions

- What is IEC 62443-4-2 used for?**
IEC 62443-4-2 defines technical security requirements for components within industrial automation and control systems (IACS). The standard is designed to help manufacturers, integrators, and asset owners protect industrial devices, such as controllers and network equipment, from cyber threats.
- Is IEC 62443-4-2 a mandatory or certifiable standard?**
IEC 62443-4-2 is not legally mandatory, but adherence is often required through contractual obligations or sector-specific regulations. While direct certification may not always be available for all components, conformance assessments and third-party validations are commonly performed to demonstrate compliance.
- What systems or organizations are in scope for IEC 62443-4-2?**
IEC 62443-4-2 applies to product manufacturers and organizations deploying industrial control system components within sectors such as energy, manufacturing, and critical infrastructure. The scope covers embedded devices, network components, host systems, and software applications integral to IACS environments.
- What are the key concepts and artifacts required by IEC 62443-4-2?**
Key concepts include mapping security capabilities to specific Security Levels (SL1-SL4), addressing requirement families like authentication, access control, confidentiality, and integrity. Required artifacts may include control documentation, security requirement mappings, test reports, and compliance evidence.
- How does implementation of IEC 62443-4-2 work in practice?**
Implementation involves integrating the standard's security controls into product development lifecycles, conducting risk assessments, documenting security features, and performing vulnerability testing. Conformance is typically verified through technical assessments and aligning with related standards such as IEC 62443-4-1 for secure development processes.

How does IEC 62443-4-2 relate to other cybersecurity frameworks?

IEC 62443-4-2 is part of the broader IEC 62443 series and complements frameworks such as IEC 62443-3-3, NIST Cybersecurity Framework, and ISO 27001. Organizations often leverage it in combination with these standards to build comprehensive, layered security programs for industrial environments.

What are the ongoing compliance requirements for IEC 62443-4-2?

Maintaining compliance requires continuous monitoring of security controls, regular vulnerability management, timely patching, and evidence of conformance through documentation and testing. Periodic reviews and updates to processes and controls ensure protection against evolving cyber threats.

How would SmartSuite support IEC 62443-4-2?

SmartSuite enables organizations to manage IEC 62443-4-2 compliance by maintaining control libraries mapped to Security Levels, tracking risks, collecting and storing compliance evidence, and facilitating remediation workflows. The platform also supports audit readiness and provides reporting dashboards for continuous oversight of security controls and governance.

License included / downloadable: No IEC 62443-4-2 is published by the International Electrotechnical Commission. Access to the full standard typically requires purchasing official documentation through authorized standards organizations. License not included with platform

Full framework page and mappings: smartsuite.com/frameworks/iec-62443-4-2-security-for-industrial-automation-and-control-systems-iacs