# ISA/IEC 62443 – Security for Industrial Automation and Control Systems (IACS)

ISA/IEC 62443 is the international series of standards for securing industrial automation and control systems across asset owners, integrators, and product suppliers.

## What it is

ISA/IEC 62443 is a series of standards that defines requirements and processes for securing industrial automation and control systems (IACS) throughout their lifecycle. It covers the hardware, software, and networks behind distributed control systems, programmable logic controllers, SCADA, and related operational technology, and it is the only consensus-based cybersecurity standard series developed specifically for automation and control applications.

The series is developed jointly by the ISA99 committee of the International Society of Automation (ISA) and Working Group 10 of IEC Technical Committee 65. ISA publishes each part as ISA-62443-x-y and the International Electrotechnical Commission (IEC) publishes the identical text as IEC 62443-x-y. In 2021 IEC designated the series a horizontal standard, meaning it applies across industries rather than to one sector. It binds through procurement, regulation, and certification: asset owners cite it in requirements, regulators reference it for critical infrastructure, and conformity assessment programs such as ISASecure and IECEE certify against it.

## At a glance

| | | |
|---|---|---|
| PUBLISHER<br>International Electrotechnical Commission (IEC) with the International Society of Automation (ISA) | TYPE<br>Standard | VERSION<br>Series; current parts 2007–2025 (IEC 62443-2-1:2024 latest revision) |
| EFFECTIVE<br>2024 (IEC 62443-2-1 edition 2) | DOMAIN<br>Cybersecurity | FAMILY<br>ISO Industry Standards |
| REGION<br>International | INDUSTRY<br>Critical Infrastructure | ADOPTION MODEL<br>Industry Requirement |
| IMPLEMENTATION COMPLEXITY<br>High | | |

Source: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

## Why it matters

- **Purpose-built for operational technology** Requirements account for legacy equipment, real-time constraints, and safety interlocks that IT-centric standards do not address.
- **Shared responsibility across the supply chain** Separate parts define what asset owners, integrators, and product suppliers must each deliver, so obligations are clear in procurement and contracts.
- **Risk-based security levels** Zones, conduits, and security levels SL 1 to SL 4 let organizations match protection to the consequence of compromise instead of applying one blanket standard.
- **Regulatory and certification recognition** The series is a horizontal IEC standard referenced by critical infrastructure

## How SmartSuite supports IEC 62443

### IEC 62443 Requirements Library

Hold the requirements of parts 2-1, 2-4, 3-3, 4-1, and 4-2 as structured records grouped by foundational requirement and security level.

### Ownership, Cadence, and Accountability

Assign each requirement and each zone to an owner with review dates so security programs stay current across sites.

### Evidence Collection and Audit Trail

Attach configuration evidence, test reports, and supplier certificates to requirements with timestamps for certification audits.

### Security Level Testing

Record target and achieved security levels per zone and track verification results against IEC 62443-3-3 requirements.

### Risk and Supplier Alignment

Link zone risk assessments and supplier or integrator obligations under 62443-2-4 and 4-1 to the controls they support.

### OT Security Reporting

Report security-level attainment, open gaps, and patch status by plant, zone, and supplier for leadership and auditors.

## Common framework mappings

IEC 62443-4-2 | ISO 27001:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5 | NIST 800-82 Rev.3 Moderate OT | NERC CIP | EU CRA | NIS2 (EU 2022/2555) | OTCC-1:2022

## Official resources

### ISA/IEC 62443 Series of Standards

ISA's overview of the series, its parts, development by ISA99 and IEC TC65, and the roles it addresses.

isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

### IEC 62443-2-1:2024 Standard

Security program requirements for IACS asset owners, edition 2, on the IEC Webstore.

webstore.iec.ch/en/publication/62883

### IEC 62443-3-3:2013 Standard

System security requirements and security levels, organized by the seven foundational requirements, on the IEC Webstore.

webstore.iec.ch/en/publication/7033

### IEC 62443-4-1:2018 Standard

Secure product development lifecycle requirements for IACS product suppliers, on the IEC Webstore.

webstore.iec.ch/en/publication/33615

## Frequently asked questions

### What is the ISA/IEC 62443 series?

ISA/IEC 62443 is a series of international standards for the cybersecurity of industrial automation and control systems, covering the hardware, software, and networks behind DCS, PLC, SCADA, and related operational technology. It defines requirements for security programs, system design, and product development across the full lifecycle, and IEC designated it a horizontal standard in 2021 so that it applies across industries.

### Who publishes IEC 62443, and how do the ISA and IEC editions differ?

The series is developed jointly by the ISA99 committee of the International Society of Automation and Working Group 10 of IEC Technical Committee 65. ISA publishes each part as ISA-62443-x-y and IEC publishes the identical text as IEC 62443-x-y, with both editions released at the same time. The content is the same; only the publisher and purchase channel differ.

### What are the main parts of IEC 62443?

The series has four groups: General (1-x) for terminology and models; Policies and Procedures (2-x), including 2-1 for asset owner security programs and 2-4 for service providers; System (3-x), including 3-2 for risk assessment with zones and conduits and 3-3 for system security requirements and security levels; and Component (4-x), including 4-1 for the secure product development lifecycle and 4-2 for technical component requirements.

### What are security levels, zones, and conduits in IEC 62443?

Zones are groupings of assets that share security requirements, and conduits are the communication paths between zones. Each zone is assigned a target security level from SL 1, protection against casual or coincidental violation, to SL 4, protection against sophisticated attackers with extended resources. IEC 62443-3-3 and 4-2 then specify the technical capabilities a system or component must have to achieve each level.

### Who needs to comply with IEC 62443?

The series applies to asset owners who operate industrial control systems, to integrators and service providers who design, install, and maintain them, and to product suppliers who develop their components. It is voluntary in itself but is widely required through procurement contracts, referenced by critical infrastructure regulators, and used as the basis for product and process certification.

### Can organizations and products be certified to IEC 62443?

Yes. ISASecure, a subsidiary of ISA, certifies development organizations to IEC 62443-4-1, components to IEC 62443-4-2, and systems to IEC 62443-3-3 through ISO/IEC 17065 accredited certification bodies, and offers site assessments aligned with 62443-2-1 and 2-4. The IECEE conformity assessment system also operates an industrial cybersecurity certification scheme for the series.

### How would SmartSuite support IEC 62443?

SmartSuite lets teams hold the IEC 62443 requirements as a control library organized by part, foundational requirement, and security level, record each zone and conduit with its target and achieved level, and link requirements to assets, suppliers, and owners. Evidence, test results, patch records, and supplier certifications attach to the same records, and dashboards show security-level attainment and open gaps by plant and zone.

License included / downloadable: No Each part of IEC 62443 is a copyrighted standard purchased from the IEC Webstore or from ISA, and the text is not included with the platform.

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