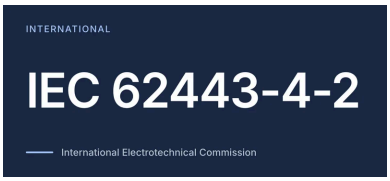
SmartSuite

Framework / Cybersecurity / ISO Industry Standards

IEC 62443-4-2:2019

IEC 62443-4-2:2019 sets technical security requirements for IACS components, with seven foundational requirements and security levels 1 to 4.



What it is

IEC 62443-4-2:2019 is the international standard for the technical security requirements of the components used in industrial automation and control systems (IACS): software applications, embedded devices, host devices and network devices. The IEC published Edition 1.0 on 27 February 2019, with a corrigendum in August 2022. Product suppliers use it to design and certify components, and system integrators and asset owners use it to specify and buy them.

It is part 4-2 of the IEC 62443 series, prepared by IEC technical committee 65, and ISA publishes the same text as ANSI/ISA-62443-4-2-2018. Its component requirements (CRs) derive from the system requirements of IEC 62443-3-3, which in turn rest on the seven foundational requirements (FRs) of IEC TS 62443-1-1. The standard defines the capability security level of a component, SL-C(component); target and achieved security levels are out of scope (clause 1).

At a glance

PUBLISHER
International Electrotechnical Commission (IEC); also published by ISA as ANSI/ISA-62443-4-2-2018

TYPE
Framework

VERSION
IEC 62443-4-2:2019, Edition 1.0 (with corrigendum COR1:2022)

EFFECTIVE
February 27, 2019

DOMAIN
Cybersecurity

FAMILY
ISO Industry Standards

REGION
International

INDUSTRY
Critical Infrastructure

ADOPTION MODEL
Industry Requirement

IMPLEMENTATION COMPLEXITY
High

Source: webstore.iec.ch/en/publication/34421

Why it matters

- **Requirements a supplier can build to** Clauses 5 to 11 set out component requirements (CR 1.1 to CR 7.8), each with rationale, requirement enhancements and security levels.
- **A buying specification** System integrators use the standard to specify the security capability level they need from each component when they procure control system components (0.2).
- **Availability protected** The first common component security constraint, CCSC 1, is support of essential functions (4.2), in line with the Introduction's point that countermeasures should not cause loss of essential services.
- **Four component types covered** Clauses 12 to 15 add software application (SAR), embedded device (EDR), host device (HDR) and network device (NDR) requirements.

© 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports IEC 62443-4-2

Component Requirements Library

Hold CR 1.1 to CR 7.8 and their requirement enhancements, grouped by foundational requirement (FR 1 to FR 7) and security level.

Component Type Register

Record whether each component is a software application, embedded device, host device or network device, and apply the SAR, EDR, HDR or NDR set that goes with it.

Security Level Target and Claim

Record the SL-C required for each component and the SL-C the supplier claims, per zone, with the gap and the owner.

Compensating Countermeasure Log

Document any compensating countermeasure used where a component cannot meet a requirement natively (CCSC 2), with approver and review date.

Verification and Test Evidence

Attach functional test results, vulnerability testing and ISASecure CSA or IEC TS 62443-6-2 evaluation evidence to each requirement.

Supplier and Certificate Tracking

Track supplier documentation, certificate scope and expiry for each component, and report open gaps by plant and zone.

Common framework mappings

ISO 27001:2022 | NIST CSF 2.0 | NERC CIP

Official resources

IEC 62443-4-2:2019 on the IEC Webstore

Edition 1.0 of the technical security requirements for IACS components, published 27 February 2019, with the August 2022 corrigendum noted.

webstore.iec.ch/en/publication/34421

IEC TS 62443-6-2:2025 on the IEC Webstore

Security evaluation methodology for components assessed against IEC 62443-4-2, published 21 January 2025.

webstore.iec.ch/en/publication/67463

Frequently asked questions

What does IEC 62443-4-2 cover, and which edition is current?

IEC 62443-4-2:2019 sets technical security requirements for the components of an industrial automation and control system: software applications, embedded devices, host devices and network devices. Edition 1.0 was published on 27 February 2019 and a corrigendum followed in August 2022. The IEC webstore lists a stability date of 2027 and no newer edition.

What are the seven foundational requirements in IEC 62443-4-2?

They are identification and authentication control (FR 1), use control (FR 2), system integrity (FR 3), data confidentiality (FR 4), restricted data flow (FR 5), timely response to events (FR 6) and resource availability (FR 7), each described in clauses 5 to 11 as a group of component requirements (CR 1.1 to CR 7.8).

How does IEC 62443-4-2 use security levels?

The standard defines the capability security level of a component, SL-C(component), from the requirements and enhancements it meets; Annex B maps each one to SL 1 to SL 4. Target levels and achieved levels of a system are out of scope. ISAGCA's guide describes SL 1 as protection against casual or coincidental violation and SL 4 as protection against intentional violation using sophisticated means with extended resources.

Can a product be certified to IEC 62443-4-2?

Yes, through ISASecure CSA (Component Security Assurance), whose version 1.0.0 took effect on 28 August 2019. A supplier must pass a security development lifecycle assessment for components, and the certification adds artifact, functional security and vulnerability identification evaluations. IEC TS 62443-6-2:2025 separately specifies an evaluation methodology for components against the standard.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What are the common component security constraints?

Clause 4 sets four constraints that apply to every component: support of essential functions (CCSC 1), compensating countermeasures (CCSC 2), least privilege (CCSC 3) and software development process (CCSC 4). They sit alongside the requirements for each foundational requirement.

License included / downloadable: No IEC 62443-4-2 is a copyrighted standard sold by the IEC and by ISA, and its text is not included with the platform.

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