SLOVENSKI STANDARD
SIST EN IEC 62443-4-2:2019/oprAA:2026

01-maj-2026

Zaščita za sisteme industrijske avtomatizacije in nadzornih sistemov - 4-2. del: Zahteve za tehnično varnost zaščito za komponente ACS

Security for industrial automation and control systems - Part 4-2: Technical security requirements for ACS components

Industrielle Kommunikationsnetze - IT-Sicherheit für industrielle Automatisierungssysteme - Teil 4-2: Technische Sicherheitsanforderungen an Komponenten industrieller Automatisierungssysteme (IACS)

Sécurité des systèmes d'automatisation et de commande industrielles - Partie 4-2: Exigences de sécurité technique des composants IACS

Ta slovenski standard je istoveten z: **EN IEC 62443-4-2:2019/prAA:2026**

ICS:

25.040.01	Sistemi za avtomatizacijo v industriji na splošno	Industrial automation systems in general
35.030	Informacijska varnost	IT Security

SIST EN IEC 62443-4-2:2019/oprAA:2026 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
EN IEC 62443-4-2:2019

prAA

March 2026

ICS 25.040.40; 35.030 -

English Version

Security for industrial automation and control systems - Part 4-2: Technical security requirements for ACS components

Sécurité des systèmes d'automatisation et de commande industrielles - Partie 4-2: Exigences de sécurité technique des composants IACS

Industrielle Kommunikationsnetze - IT-Sicherheit für industrielle Automatisierungssysteme - Teil 4-2: Technische Sicherheitsanforderungen an Komponenten industrieller Automatisierungssysteme (IACS)

This draft amendment prAA, if approved, will modify the European Standard EN IEC 62443-4-2:2019; it is submitted to CENELEC members for enquiry.
Deadline for CENELEC: 2026-06-05.

It has been drawn up by CLC/TC 65X.

If this draft becomes an amendment, CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this amendment the status of a national standard without any alteration.

This draft amendment was established by CENELEC in three official versions (English, French, German).
A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Contents

Page

European foreword

This document (EN IEC 62443-4-2:2019/prAA:2026) has been prepared by CLC/TC 65X “Industrial-process measurement, control and automation”.

This document is currently submitted to the Enquiry.

The following dates are proposed:

• latest date by which the existence of this document has to be announced at national level	(doa)	dav + 6 months
• latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	dav + 12 months
• latest date by which the national standards conflicting with this document have to be withdrawn	(dow)	dav + 36 months (to be confirmed or modified when voting)

This document will amend EN IEC 62443-4-2:2019.

EN IEC 62443-4-2:2019/prAA:2026 includes the following significant technical modifications with respect to EN IEC 62443-4-2:2019:

— update of existing requirements and introduction of new requirements;

— update by introducing a full evaluation methodology;

— updates of requirements to include requirement-specific applicability criteria, acceptance criteria and evaluation artefacts.

This document has been prepared under a standardization request addressed to CENELEC by the European Commission. The Standing Committee of the EFTA States subsequently approves these requests for its Member States.

For the relationship with EU Legislation, see informative Annex ZZ, which is an integral part of this document.

Introduction

The purpose of this amendment is to identify and modify the requirements and associated clauses to align with the EU Cyber Resilience Act essential cybersecurity requirements, so that the amendment (EN IEC 62443-4-2:2019/prAA:2025), once made available by CENELEC, can be offered for citation under the Cyber Resilience Act.

1 Modification to the title

Replace the title with the following:

"Security for industrial automation and control systems - Part 4-2: Technical security requirements for ACS components"

2 Modification to the Introduction

2.1 Modification to Subclause 0.1, "Overview"

Replace the whole content of "0.1 Overview" with the following:

"This document defines cybersecurity technical requirements for components used in operational technology (OT) environments. OT is the technology for detecting, managing or causing change through the monitoring or control of physical entities – for example sensors, actuators, programmable logic controllers (PLCs), industrial communication devices, supervisory control systems and related software applications.

These requirements can support interested parties (e.g. during conformity assessment activities) to achieve comparability of assessment results. Annex B introduces a security evaluation methodology that integrates lifecycle-based practices with component-level assurance criteria."

2.2 Modification to Subclause 0.2, "Purpose and intended audience"

Replace the whole content of "0.2 Purpose and intended audience" with the following:

"This document is intended for product suppliers, but also other interested parties involved in the development, integration, testing, and assessment of automation and control system components. Relevant stakeholders include, but are not limited to, security engineers, software and hardware developers, system architects, product managers, test engineers, compliance and regulatory personnel, security incident response personnel, and documentation personnel.

This document helps product suppliers to understand the security requirements placed on ACS components. An ACS component might not provide a required capability itself but might be designed to integrate with a higher-level entity and thus benefit from that entity's capability – for example a device might not be maintaining a user directory itself but might integrate with a system wide authentication and authorization service and thus still meet the requirements to provide individual user authentication, authorization and management capabilities. This document will guide product suppliers as to which requirements can be allocated and which requirements should be native in the components."

3 Modification to Clause 1, "Scope"

Replace the whole content of "Scope" with the following:

"This document provides detailed technical control system component requirements (CRs) associated with the seven foundational requirements (FRs) including defining the requirements for automation control systems capability security levels and their components, SL-C(component).

The seven foundational requirements (FRs) are:

a) identification and authentication control (IAC),

b) use control (UC),

c) system integrity (SI),

d) data confidentiality (DC),

e) restricted data flow (RDF),

f) timely response to events (TRE), and

g) resource availability (RA).

These seven foundational requirements provide a basis for the technical security requirements in this document. The first of these, FR-1, addresses the capabilities necessary to reliably identify and authenticate all users (humans, software processes, and devices) attempting to access the component. FR-2 addresses the capabilities necessary to enforce the assigned privileges of an authenticated user (human, software process, and device) to perform actions on a component and monitor use of these privileges. FR-3 addresses the capabilities necessary for the integrity of the component to protect against unauthorized manipulation or modification. FR-4 addresses the capabilities necessary for the confidentiality of information on communication data flows and in data stored at rest and processed by the component to prevent unauthorized disclosure. FR-5 addresses the capabilities necessary to support segmentation of networks and data flows and limit unnecessary and unwanted flow of data. FR-6 addresses the capabilities necessary to respond to security violations by notifying the proper authority, reporting needed evidence of a violation and taking timely corrective action when incidents are discovered. FR-7 addresses the capabilities necessary to protect the availability of components against the degradation or denial of essential functions and services.

Within each FR, the technical security requirements are grouped into security levels as a basis for selection of security measures as part of a risk-based approach."

4 Modification to Clause 2, "Normative references"

Replace the second normative reference with the following:

EN IEC 62443-3-3:2019, *Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels*

Replace the third normative reference with the following:

EN IEC 62443-4-1:2018,[1] *Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements*

5 Modification to Clause 3, "Terms, definitions, abbreviated terms, acronyms, and conventions"

5.1 Modification to Subclause 3.1, "Terms and definitions"

Replace the content of subclause 3.1 with the following:

"

For the purposes of this document, the terms and definitions given in EN IEC 62443-3-3:2019 and EN IEC 62443-4-1:2018, and the following apply.

NOTE Many of the following terms and definitions are originally based on relevant International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) and US. National Institute of Standards and Technology (NIST) sources, sometimes with minor modifications to enhance suitability for ACS security requirements."

[1] As impacted by EN IEC 62443-4-1:2018/prAA:2026.

Add the following term entry 3.1.1:

3.1.1
ACS component specification
list of artefacts resulting from the application of an EN IEC 62443-4-1 secure development lifecycle to an ACS component

Add the following term entry 3.1.2:

3.1.2
artefact
result of executing a secure development lifecycle or documented evidence according to the process requirements of EN IEC 62443-4-1

EXAMPLE documented threat models, definitions and descriptions of security requirements, or test case specifications and results

Note 1 to entry: Artefact is used with the same meaning as evidence but implies that the processes of EN IEC 62443-4-1 were applied to the product.

[SOURCE: CLC IEC/TS 62443-6-2:2025]

Replace the clause number of term entry "asset" to 3.1.3 from 3.1.1 and replace "IACS" with "ACS".

Replace clause number of term entry "asset owner" to 3.1.4 from 3.1.2 and replace "IACS" with "ACS".

Replace the clause number of term entry "attack" to 3.1.5 from 3.1.3 and replace "IACS" with "ACS".

Add the following term entry 3.1.6:

3.1.6
authenticated security test
security test allowing a tester direct access to products or components using remote administrative protocols and to authenticate to the products or components using provided credentials

EXAMPLE Secure shell (SSH) or remote desktop protocol (RDP) are examples of remote administrative protocols

Note 1 to entry: Authenticated security tests provide a more thorough view and more detailed insights of the tested product compared to unauthenticated security tests. They can therefore identify additional vulnerabilities at the product which had not been detected by unauthorized security tests.

Replace the clause number of term entry "authentication" to 3.1.7 from 3.1.4.

Replace the clause number of term entry "authenticator" to 3.1.8 from 3.1.5.

Replace the clause number of term entry "authenticator" to 3.1.9 from 3.1.6.

Add the following term entry 3.1.10:

3.1.10
automation and control system
collection of integrated components that provide functions for monitoring, controlling and managing the operation of equipment under control

Add the following term entry 3.1.11:

3.1.11
automation and control system component
component developed and supported according to the secure development processes described in EN IEC 62443-4-1 and implementing the applicable technical requirements of EN IEC 62443-4-2

Replace the clause number of term entry "availability" to 3.1.12 from 3.1.7.

Add the following term entry 3.1.13:

3.1.13
check
generate a verdict by a simple comparison

[SOURCE: ISO/IEC 18045:2022, 3.1]

Replace the clause number of term entry "communication channel" to 3.1.14 from 3.1.8.

Replace the clause number of term entry "compensating countermeasure" to 3.1.15 from 3.1.9 and replace "IACS" with "ACS".

Replace the clause number of term entry "component" to 3.1.16 from 3.1.10.

Replace the clause number of term entry "conduit" to 3.1.17 from 3.1.11.

Replace the clause number of term entry "confidentiality" to 3.1.18 from 3.1.2 and replace "IACS" with "ACS".

Replace the clause number of term entry "conduit" to 3.1.19 from 3.1.13.

Replace the clause number of term entry "control system" to 3.1.20 from 3.1.14 and replace "IACS" with "ACS".

Replace the clause number of term entry "compensating countermeasure" to 3.1.21 from 3.1.15.

Replace the clause number of term entry "degraded mode" to 3.1.22 from 3.1.16.

Replace the clause number of term entry "device" to 3.1.23 from 3.1.17.

Replace the clause number of term entry "embedded device" to 3.1.24 from 3.1.18.

Replace the clause number of term entry "environment" to 3.1.25 from 3.1.19 and replace "IACS" with "ACS".

Add the following term entry 3.1.26:

3.1.26
equipment under control
equipment, machinery, apparatus, or plant used for manufacturing, process, transportation, medical, or other activities

[SOURCE: IEC 61508-4:2010]

Replace the clause number of term entry "essential function" to 3.1.27 from 3.1.20.

Add the following term entry 3.1.28:

3.1.28
evaluation
systematic determination of the extent to which the target of evaluation meets its specified requirements by either a check (3.1.13) or examine (3.1.33)

Note 1 to entry: In the EN IEC 62443 series evaluation is used during conformity assessment.

[SOURCE: CLC IEC/TS 62443-6-2:2025]

Add the following term entry 3.1.29:

3.1.29
evaluation activity
determination if the target of evaluation meets the referenced requirements of the standard

[SOURCE: CLC IEC/TS 62443-6-2:2025]

Add the following term entry 3.1.30:

3.1.30
evaluation criteria
criteria used to determine whether the target of evaluation fulfils the evaluated requirement in a suitable manner

[SOURCE: CLC IEC/TS 62443-6-2:2025]

Add the following term entry 3.1.31:

3.1.31
evaluator
individual or organization that performs the evaluation

[SOURCE: ISO 25040:2011, 4.25]

Replace the clause number of term entry "event" to 3.1.32 from 3.1.21 and replace "IACS" with "ACS".

Add the following term entry 3.1.33:

3.1.33
examine
generate a verdict by analysis using evaluator expertise

[SOURCE: ISO/IEC 18045:2022, 3.9]

Add the following term entry 3.1.34:

3.1.34
external interface
physical or logical interface of a component that can be accessed from outside the component

EXAMPLE Machine, network, user interfaces, and API are types of external interfaces.

Replace the clause number of term entry "firecall" to 3.1.35 from 3.1.22.

Replace the clause number of term entry "host device" to 3.1.36 from 3.1.23.

Replace the clause number of term entry "identifier" to 3.1.37 from 3.1.24.

Replace the clause number of term entry "incident" to 3.1.38 from 3.1.25.

Delete the term entry 3.1.26 "industrial automation and control system" and replace the clause number of term entry "integrity" to 3.1.39 from 3.1.27.

Add the following term entry 3.1.40:

3.1.40
intended use
use for which a product is designed by the product supplier, describing the explicit and implicit assumptions about the product's properties and capabilities

EXAMPLE The intended use of a network switch is to switch network traffic in an enterprise environment used by skilled persons. The intended use does not describe specific product features, e.g. security update capability, authentication mechanism.

Note 1 to entry: The product security context is derived from the intended use

Replace the clause number of term entry "least privilege" to 3.1.41 from 3.1.28 and replace "IACS" with "ACS".

Replace term entry 3.1.29 "mobile code" with the following.

3.1.42
mobile code
code or script loaded, transferred or entered from a source external to the component that can be executed without explicit installation by the recipient

EXAMPLE JavaScript, VBScript, Serialized Java objects, Shell scripts and other scripting languages.

Replace the clause number of term entry "mobile device" to 3.1.43 from 3.1.30.

Replace the clause number of term entry "network device" to 3.1.44 from 3.1.31.

Replace the clause number of term entry "non-repudiation" to 3.1.45 from 3.1.32.

Add the following term entry 3.1.46:

3.1.46
operational technology
technology for detecting, facilitating, managing or causing change, through automation, monitoring or control, to a physical entity or environment

[SOURCE: IEC/TS 62443-1-1:2009]

Add the following term entry 3.1.47:

3.1.47
product
system, subsystem or component that is manufactured, developed or refined

Note 1 to entry: In the context of EN IEC 62443-3-3:2019 a product is an automation and control system (ACS).

Note 2 to entry: In the context of this document a product is an ACS component.

Add the following term entry 3.1.48:

3.1.48
product security context
security provided to the product by the environment (product user deployment) in which the product is intended to be used

Replace the clause number of term entry "product supplier" to 3.1.49 from 3.1.33.

Replace the clause number of term entry "remote access" to 3.1.50 from 3.1.34.

Replace the clause number of term entry "role" to 3.1.51 from 3.1.35 and replace "IACS" with "ACS".

Replace the clause number of term entry "safety instrumented system" to 3.1.52 from 3.1.36.

Replace term entry 3.1.37 "security level" with the following:

3.1.53
security level
set of security measures that supports a degree of risk reduction

Add the following term entry 3.1.54:

3.1.54
security test grade
defined set of security test modules

Add the following term entry 3.1.55:

3.1.55
security test module
specification of a security testing activity, describing the aim of the security test, the testing methodology and acceptance criteria

Add the following term entry 3.1.56:

3.1.56
security verification and validation testing
testing performed to assess the overall security of a component, product or system when used in its intended product security context and to determine if a component, product or system satisfies the product security requirements and satisfies its designed security purpose

Note 1 to entry: Examples for security testing according to IEC 62443-4-1 are threat mitigation testing, vulnerability testing and penetration testing.

Note 2 to entry: Security verification and validation testing is the term used in EN IEC 62443-4-1.

[SOURCE: EN IEC 62443-4-1:2018, 3.1.44, modified — the notes have been added]

Add the following term entry 3.1.57:

3.1.57
sensitive information
information and related data that needs to be protected under law or for which unavailability, disclosure, modification or loss impacts security

Replace the clause number of term entry "session" to 3.1.58 from 3.1.38.

Replace the clause number of term entry "session ID" to 3.1.59 from 3.1.39.

Replace the clause number of term entry "setpoint" to 3.1.60 from 3.1.40.

Add the following term entry 3.1.61:

3.1.61
single purpose component
dedicated device that is exclusively allocated to a single entity and single application

EXAMPLE Sensor, actuator, unmanaged network switch

Replace the clause number of term entry "software application" to 3.1.62 from 3.1.41.

Add the following term entry 3.1.63:

3.1.63
supporting measure
functions (e.g. provided by the underlying software or hardware) and procedures (e.g. to ensure physical protection) provided by the product security context to support the implementation of the component requirement

Add the following term entry 3.1.64:

3.1.64
system
interacting, interrelated, or interdependent elements forming a complex whole

Replace the clause number of term entry "system integrator" to 3.1.65 from 3.1.42.

Add the following term entry 3.1.66:

3.1.66
target of evaluation
subject of a security evaluation

Note 1 to entry: the subject of a security evaluation is a product, i.e. either an automation and control system (ACS) or an ACS component.

Replace the clause number of term entry "threat" to 3.1.67 from 3.1.43.

Add the following term entry 3.1.68:

3.1.68
time-related information
information or related data representing an absolute or relative time or that can be used to derive an absolute or relative time

Note 1 to entry: Time-related information might be the period of time, in seconds, since power up of the component, or simply the sequence of occurred events

Replace the clause number of term entry "trust" to 3.1.69 from 3.1.44.

Add the following term entry 3.1.70:

3.1.70
unauthenticated security test
security test performed without any authentication at the tested product or component

Replace the clause number of term entry "untraceability" to 3.1.71 from 3.1.45.