SLOVENSKI STANDARD
SIST EN IEC 62443-4-1:2018/oprAA:2026

01-maj-2026

Zaščita industrijske avtomatizacije in nadzornih sistemov - 4-1. del: Zahteve za varnost izdelka v obdobju razvoja izdelka

Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements

IT-Sicherheit für industrielle Automatisierungssysteme - Teil 4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung

Sécurité des automatismes industriels et des systèmes de commande - Partie 4-1 : Exigences applicables au cycle de vie de développement sécurisé des produits

Ta slovenski standard je istoveten z: **EN IEC 62443-4-1:2018/prAA:2026**

ICS:

13.020.60	Življenjski ciklusi izdelkov	Product life-cycles
25.040.01	Sistemi za avtomatizacijo v industriji na splošno	Industrial automation systems in general
35.030	Informacijska varnost	IT Security

SIST EN IEC 62443-4-1:2018/oprAA:2026 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
EN IEC 62443-4-1:2018

prAA

March 2026

ICS 35.030; 25.040.40 -

English Version

Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements

Sécurité des automatismes industriels et des systèmes de commande - Partie 4-1 : Exigences applicables au cycle de vie de développement sécurisé des produits

IT-Sicherheit für industrielle Automatisierungssysteme - Teil 4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung

This draft amendment prAA, if approved, will modify the European Standard EN IEC 62443-4-1:2018; 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

European foreword

This document (EN IEC 62443-4-1:2018/prAA:2026) has been prepared by Technical Committee 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 modify EN IEC 62443-4-1:2018 (PR = 81847).

EN IEC 62443-4-1:2018/prAA:2026 includes the following significant technical modifications with respect to EN IEC 62443-4-1:2018:

— update of existing requirements and introduction of new requirements;

— update by introducing an applicability assessment process;

— additon of new practice Risk management.

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.

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 62443-4-1:2018/prAA:2026), once made available by CENELEC, can be used as a normative reference by EN IEC 62443-4-2:2019/prAA:2026.

1 Modification to the Introduction

Replace the content of the Introduction with the following:

"This document is part of a series of standards that addresses the issue of security for automation and control systems (ACS). This document describes product development lifecycle requirements related to cyber security for products intended for use in the automation and control systems environment and provides guidance on how to meet the requirements described for each element.

This document is the part of the EN IEC 62443 series that contains security requirements for developers of any automation and control products where security is a concern."

2 Modification to Clause 1, "Scope"

Replace the content with the following:

"This part of EN IEC 62443 specifies process requirements for the secure development of products used in automation and control systems. It defines a secure development lifecycle (SDL) for the purpose of developing and maintaining secure products. This secure development lifecycle includes security risk management, security requirements definition, secure design, secure implementation (including coding guidelines), verification and validation, defect management, security update management and product end-of-life. These requirements can be applied to new or existing processes for developing, maintaining and retiring hardware, software or firmware for new or existing products. These requirements apply to the developer and maintainer of the product, but not to the integrator or product user. A summary list of the requirements in this document can be found in Annex B."

3 Modification to Clause 2, "Normative references"

Replace the reference with the following:

IEC 62443-2-4:2015,[1] *Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers*

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

4.1 Modification to Subclause 3.1, "Terms and definitions"

Replace the 1st paragraph with the following:

"For the purposes of this document, the terms and definitions given in IEC/TR 62443-1-2 [1] and the following apply."

Replace term entry 3.1.3 with the following:

[1] As impacted by IEC 62443-2-4:2015/AMD1:2017.

3.1.3
access control
<process>
process by which use of system resources is regulated according to a security policy and is permitted by only authorized product users according to that policy

Note 1 to entry: Access control includes identification and authentication requirements specified in other parts of the EN IEC 62443 series.

Replace term entry 3.1.4 with the following:

3.1.4
administrator
product user who has been authorized to manage security policies/capabilities for a product or system

Replace Note 1 to entry in 3.1.5 with the following:

Note 1 to entry: In this specific case, an asset is an object that is part of an ACS.

Delete term entry 3.1.6 "asset owner".

Replace the clause number for term entry "attack surface" to 3.1.6 from 3.1.7.

Replace the clause number of term entry "audit log" to 3.1.7 from 3.1.8.

Replace the clause number of term entry "authentication" to 3.1.8 from 3.1.9 and replace the notes to entry with the following:

Note 1 to entry: Not all credentials used to authenticate an identity are created equally. The trustworthiness of the credential is determined by the configured authentication mechanism. Hardware or software-based mechanisms can force product users to prove their identity before accessing data on a device. A typical example is proving the identity of a user usually through an identity provider.

Note 2 to entry: Authentication includes verifying human product users as well as non-human product users such as devices or processes.

Add the following term entry 3.1.9:

3.1.9
authenticated security test
test which allows the tester to directly access products using remote administrative protocols such as secure shell (SSH) or remote desktop protocol (RDP) and to authenticate to the products using provided credentials

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 term entry 3.1.10 "automation solution" with the following:

3.1.10
automation and control system
ACS
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
ACS 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

Add the following term entry 3.1.12:

3.1.12
automation and control solution
collection of people processes and automation and control systems with the purpose of monitoring, controlling and managing the operation of equipment under control

Note 1 to entry: An automation and control solution includes the instantiation of one or more automation and control systems.

Note 2 to entry: Automation and control solution is used as a proper noun in this part of the EN IEC 62443 series.

Note 3 to entry: The difference between the automation and control system and the automation and control solution is that the automation and control system is incorporated into the automation and control solution design (for example, a specific number of workstations, controllers and devices in a specific configuration), which is then implemented. The resulting configuration is referred to as the automation and control solution.

Note 4 to entry: The automation and control solution can be comprised of components from multiple suppliers including the product supplier of the automation and control system.

Replace the clause number of term entry "banned function" to 3.1.13 from 3.1.11.

Replace term entry 3.1.14 "best practices" with the following

3.1.14
best practices
guidelines for securely designing, developing, verifying and validating, maintaining or retiring products that the supplier has determined are commonly recommended by both the security and industrial automation communities

EXAMPLE least privilege, economy of mechanism and least common mechanism

Replace term entry 3.1.13 "component" with the following:

3.1.15
component

one of the parts that make up a product or system. A component may be hardware or software and may be subdivided into other components

Replace term entry 3.1.14 "configuration management" with the following:

3.1.16
configuration management
discipline of identifying the components of an evolving system for the purposes of controlling changes to those components and maintaining continuity and traceability throughout the secure product development lifecycle

Add the following term entry 3.1.17:

3.1.17
cryptographic mechanism
element of software or hardware that provides a cryptographic service, such as confidentiality, integrity, source authentication, and access control

Note 1 to enrtry: The cryptographic mechanism can be, for example, a set of cryptographic algorithms or a protocol utilizing cryptography.

Delete term entry 3.1.18 "externally provided component".

Replace the clause number of term entry "defense in depth" to 3.1.18 from 3.1.15.

Replace the clause numberi of term entry "dependent component" to 3.1.19 from 3.1.16 and replace the example with the following:

EXAMPLE Java run time environment or a driver

Delete term entry 3.1.20 "industrial automation and control system".

Replace term entry 3.1.17 "deprecated function" with the following:

3.1.20

deprecated function

software method that is supported but whose use is no longer recommended

Add the following term entry 3.1.21:

3.1.21
equipment under control
equipment, machinery, apparatus, or plant used for manufacturing, process, transportation, medical, or other activities

[SOURCE: IEC 61508-4:2010]

Add the following term entry 3.1.22:

3.1.22
essential function
function or capability that is required to maintain health, safety, the environment and availability for the equipment under control

Note 1 to entry: Essential functions include, but are not limited to, the safety instrumented function (SIF), the control function and the ability of the operator to view and manipulate the equipment under control. The loss of essential functions is commonly termed loss of protection, loss of control and loss of view respectively. In some industries additional functions such as history may be considered essential.

Replace the clause number of term entry "fuzz testing" to 3.1.23 from 3.1.19.

Add the following term entry 3.1.24:

3.1.24
information category
logical grouping of information that shares a common purpose and set of security requirements

Add the following term entry 3.1.25:

3.1.25
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

Note 1 to entry: The intended use does not describe specific product features, e.g. security update capability, authentication mechanism.

EXAMPLE The intended use of a network switch is to switch network traffic in an enterprise environment used by skilled persons.

Replace term entry 3.1.22 "product" with the following:

3.1.26
product
system, subsystem or component that is manufactured, developed or refined

Note 1 to entry: in the context of EN IEC 62443-3-3 [4] a product is an automation and control system (ACS)

Note 2 to entry: in the context of EN IEC 62443-4-2 [5] a product is an ACS component

Replace term entry 3.1.23 "configuration management" with the following:

3.1.27
product security context
security provided to the product by the environment (product user deployment) in which the product is intended to be used

Note 1 to entry: The security provided to the product by its intended environment can effectively restrict the threats that are applicable to the product.

Note 2 to entry: The product security context is derived from the intended use.

Add the following term entry 3.1.28:

3.1.28
product security context category
structural categorization describing the product security context through different factors to support comparable assumptions about the product's security context

Add the following term entry 3.1.29:

3.1.29
product security incident
security compromise that has a measurable impact on the product user, or an attempted compromise that, if successful, would have resulted in a measurable impact on the product user

Replace the clause number of term entry "product supplier" to 3.1.30 from 3.1.24.

Replace term entry 3.1.25 "product users" with the following:

3.1.31
product user
user of the hardware and/or software product including administrator, integrator and maintenance personnel, and vendor of other components or products that reuse or contain this product

Replace the clause number of term entry "record" to 3.1.32 from 3.1.26.

Replace the clause number of term entry "regression" to 3.1.33 from 3.1.27.

Add the following term entry 3.1.34:

3.1.34
review
activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives

[SOURCE: ISO 31073:2022, 3.3.41]

Replace the clause number of term entry "root cause" to 3.1.35 from 3.1.28.

Add the following term entry 3.1.36:

3.1.36
secure by default
state of the product being securely configured upon installation or deployment according to its intended use and product security context

Replace the clause number of term entry "security defect" to 3.1.37 from 3.1.29.

Replace term entry 3.1.30 "security advisor" with the following:

3.1.38
security advisor
organizational role to guide team in the process of the SDL (Security Development Lifecycle)

Note 1 to entry: Security advisor may be part of the project team or may be consultant to the team to provide guidance and assistance where required.

Replace the clause number of term entry "security-related issue" to 3.1.39 from 3.1.32 and add the following example:

EXAMPLE A product vulnerability is a type of security-related issue.

Add the following term entry 3.1.40:

3.1.40
security support period
period during which a product supplier ensures that security support processes are active and security issues in the product are handled

Note 1 to entry: The length and obligations of security support can be pre-determined by regulatory or contractual terms.

Add the following term entry 3.1.41:

3.1.41
security test grade
STG
defined set of security test modules.

Note 1 to entry: Security test grades are STG-1, STG-2, STG-3, and STG-4.

Add the following term entry 3.1.42:

3.1.42
security test module
STM
specification of a security testing activity, describing the aim of the security test, the testing methodology and acceptance criteria.

Replace term entry 3.1.21 "patch management" with the following:

3.1.43
security update management
area of systems management that involves acquiring, testing and installing software security updates (code changes) to a product

Note 1 to entry: See IEC/TR 62443-2-3 [2] for additional information.

Note 2 to entry: Security update management also applies to the process of keeping included 3rd party libraries current before releasing a product.

Replace term entry 3.1.33 "security-related issue" with the following:

3.1.44
security verification and validation testing
testing performed to assess the overall security of a component or product when used in its intended product security context and to determine if a component or product satisfies the product security requirements and satisfies its designed security purpose

Note 1 to entry: Security verification testing supplements security validation testing with additional testing focused on the product security context and defence in depth strategy

Add the following term entry 3.1.45:

3.1.45
software bill of materials (SBOM)
information in a structured format that allows the exchange of information for a software package, which might usefully include name, version, origin, license, copyright and known vulnerabilities in a manner useful to third parties

[SOURCE: ISO/IEC 18974:2023(en), 3.12, modified — a reference to SPDX as possible format was removed]

Add the following term entry 3.1.46:

3.1.46
supporting measure
functions and procedures external to the product to support the implementation of the product security requirements

Note 1 to entry: Functions are e.g. provided by the underlying software or hardware.

Note 2 to entry: Procedures have e.g. the aim to ensure physical protection.

Add the following term entry 3.1.47:

3.1.47
system
interacting, interrelated, or interdependent elements forming a complex whole

Replace the clause number of term entry "system integrator" to 3.1.48 from 3.1.34.

Add the following term entry 3.1.49:

3.1.49
test
activity in which a system or component is executed under specified conditions, the results are observed or recorded, and an evaluation is made of some aspect of the system or component

Note 1 to entry: A test is carried out to measure or classify a characteristic or a property of an item by applying to the item a set of environmental and operating conditions and/or requirements.

[SOURCE: ISO/IEC/IEEE 29119-2:2021, 3.21]

Add the following term entry 3.1.50:

3.1.50
third-party component
component included in a product that is developed and maintained by a third-party supplier.

Note 1 to entry: This includes components which are specifically developed by a third-party supplier for the product supplier.

Replace term entry 3.1.35 "third-party supplier" with the following:

3.1.51
third-party supplier
organization independent of the product supplier organization

Note 1 to entry: A third-party supplier can also mean a different legal entity of the corporation the product supplier organization belongs to.

Replace the clause number of term entry "threat" to 3.1.52 from 3.1.36.

Replace the clause number of term entry "threat modelling" to 3.1.53 from 3.1.37.

Add the following term entry 3.1.54:

3.1.54
threat scenario
description of how a threat, exploiting one or more vulnerabilities could trigger an incident leading to adverse impact

Replace the clause number of term entry "trust boundary" to 3.1.55 from 3.1.38.

Add the following term entry 3.1.56:

3.1.56
unauthenticated security test
unauthenticated security tests are security tests performed without any authentication at the tested products.

Replace term entry 3.1.39 "unit testing" with the following:.

3.1.57
unit testing
verification that an individual unit of computer software or hardware performs as intended

Note 1 to entry: Automated verification, or testing, is generally performed by computer test software.

Note 2 to entry: What constitutes a unit of source code is a design decision. A unit is often designed as the smallest testable part of an application. It may include one or more computer program modules and may also include associated control data, usage procedures and operating procedures. In procedural programming, a unit could be an entire module but is more commonly an individual function or procedure. In object-oriented programming, a unit is often an entire interface, such as a class, but could be an individual method.

Replace the clause number of term entry "user" to 3.1.58 from 3.1.40.

Replace the clause number of term entry "zone" to 3.1.59 from 3.1.41.

4.2 Modification to Subclause 3.2, "Abbreviated terms and acronyms"

Replace the list of abbreviated terms and acronyms with the following:

ACL	Access control list
ACS	Automation control system
CMMI	Capability maturity model integration
CMMI-DEV	Capability maturity model integration for development
CMU	Carnegie Mellon University
COTS	Commercial off the shelf
CVSS	Common vulnerability scoring system
DAST	Dynamic application security testing
DM	Defect management
FDIS	Final Draft International Standard
HTTP	Hypertext transfer protocol
IEC	International Electrotechnical Commission
ISA	International Society of Automation
ISO	International Organization for Standardization
MIN	Minimum
OWASP	Open Web Application Security Project
QA	Quality assurance
SAST	Static Application Security Testing
SL-C	Capability Security Level
SD	Secure Design
SDL	Security development lifecycle
SDLA	Secure Development Lifecycle Assessment
SEI	Software Engineering Institute
SG	Security guidelines
SI	Secure implementation
SL	Security level
SL-C	Capability security level
SM	Security management
SR	Security requirements
STG	Security test grade