SLOVENSKI STANDARD
SIST EN IEC 62443-2-4:2024

01-september-2024

Zaščita industrijske avtomatizacije in nadzornih sistemov - 2-4. del: Zahteve za program zaščite za ponudnike storitev IACS (IEC 62443-2-4:2023)

Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers (IEC 62443-2-4:2023)

IT-Sicherheit für industrielle Automatisierungssysteme - Teil 2-4: Anforderungen an das IT-Sicherheitsprogramm von Dienstleistern für industrielle Automatisierungssysteme (IEC 62443-2-4:2023)

Sécurité des automatismes industriels et des systèmes de commande - Partie 2-4: Exigences de programme de sécurité pour les fournisseurs de service IACS (IEC 62443-2-4:2023)

Ta slovenski standard je istoveten z: **EN IEC 62443-2-4:2024**

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 62443-2-4:2024 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN IEC 62443-2-4

January 2024

ICS 25.040.40; 35.100.05

Supersedes EN IEC 62443-2-4:2019;
EN IEC 62443-2-4:2019/A1:2019

English Version

Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers (IEC 62443-2-4:2023)

Sécurité des automatismes industriels et des systèmes de commande - Partie 2-4: Exigences de programme de sécurité pour les fournisseurs de service IACS
(IEC 62443-2-4:2023)

IT-Sicherheit für industrielle Automatisierungssysteme - Teil 2-4: Anforderungen an das IT-Sicherheitsprogramm von Dienstleistern für industrielle Automatisierungssysteme
(IEC 62443-2-4:2023)

This European Standard was approved by CENELEC on 2024-01-19. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists 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.

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

European foreword

The text of document 65/1021/FDIS, future edition 2 of IEC 62443-2-4, prepared by IEC/TC 65 "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 62443-2-4:2024.

The following dates are fixed:

• latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2024-10-19
• latest date by which the national standards conflicting with the document have to be withdrawn	(dow)	2027-01-19

This document supersedes EN IEC 62443-2-4:2019 and all of its amendments and corrigenda (if any).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users' national committee. A complete listing of these bodies can be found on the CENELEC website.

Endorsement notice

The text of the International Standard IEC 62443-2-4:2023 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standard indicated:

IEC 62682:2022	NOTE Approved as EN IEC 62682:2023 (not modified)
ISO/IEC 30111	NOTE Approved as EN ISO/IEC 30111
ISO 15189:2022	NOTE Approved as EN ISO 15189:2022 (not modified)

IEC 62443-2-4

Edition 2.0 2023-12

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers

Sécurité des automatismes industriels et des systèmes de commande – Partie 2-4: Exigences de programme de sécurité pour les fournisseurs de service IACS

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 25.040.40, 35.100.05

ISBN 978-2-8322-7779-9

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 2-4: Security program requirements for IACS service providers

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

9) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch. IEC shall not be held responsible for identifying any or all such patent rights.

This document has been prepared by of IEC technical committee 65: Industrial-process measurement, control and automation in collaboration with the liaison International Instrumentation Users Association, referred to as the WIB from its original and now obsolete Dutch name. It is an International Standard.

This publication contains an attached file in the form of a .CSV spreadsheet version of Table A.1. This file is intended to be used as a complement and does not form an integral part of the publication.

This second edition cancels and replaces the first edition published in 2015 and Amendment 1:2017. This edition constitutes a technical revision.

This edition contains editorial updates and clarifications and does not contain significant technical changes with respect to the previous edition. One area of clarification is that some of the requirements could have been interpreted as requirements for technical capabilities. These requirements were clarified so that they are expressed as requirements for the use/configuration of technical capabilities.

The text of this International Standard is based on the following documents:

Draft	Report on voting
65/1021/FDIS	65/1029/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

A list of all parts in the IEC 62443 series, published under the general title *Security for industrial automation and control systems*, can be found on the IEC website.

Future standards in this series will carry the new general title as cited above. Titles of existing standards in this series will be updated at the time of the next edition.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

IMPORTANT – The "colour inside" logo on the cover page of this document indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 2-4: Security program requirements for IACS service providers

1 Scope

This part of IEC 62443 specifies a comprehensive set of requirements for security-related processes that IACS service providers can offer to the asset owner during integration and maintenance activities of an Automation Solution. Because not all requirements apply to all industry groups and organizations, Subclause 4.1.4 provides for the development of "profiles" that allow for the subsetting of these requirements. Profiles are used to adapt this document to specific environments, including environments not based on an IACS.

NOTE 1 The term "Automation Solution" is used as a proper noun (and therefore capitalized) in this document to prevent confusion with other uses of this term.

Collectively, the security processes offered by an IACS service provider are referred to as its Security Program (SP) for IACS asset owners. In a related specification, IEC 62443-2-1 describes requirements for the Security Management System of the asset owner.

NOTE 2 In general, these security capabilities are policy, procedure, practice and personnel related.

Figure 1 illustrates the integration and maintenance security processes of the asset owner, service provider(s), and product supplier(s) of an IACS and their relationships to each other and to the Automation Solution. Some of the requirements of this document relating to the safety program are associated with security requirements described in IEC 62443-3-3 and IEC 62443-4-2.

NOTE 3 The IACS is a combination of the Automation Solution and the organizational measures necessary for its design, deployment, operation, and maintenance.

NOTE 4 Maintenance of legacy system with insufficient security technical capabilities, implementation of policies, processes and procedures can be addressed through risk mitigation.

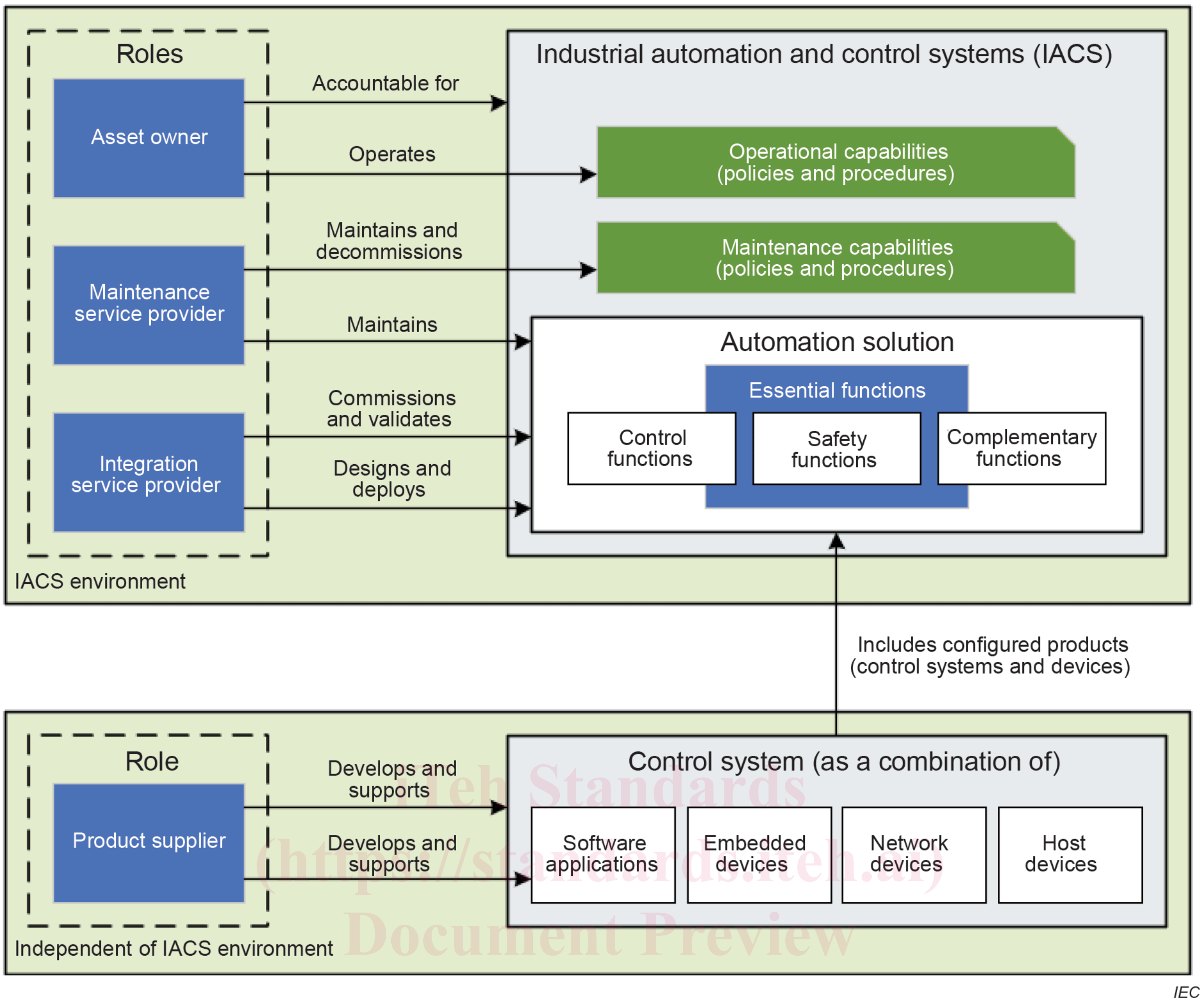
Roles
Asset owner
Maintenance service provider
Integration service provider
Accountable for
Operates
Maintains and decommissions
Maintains
Commissions and validates
Designs and deploys
Industrial automation and control systems (IACS)
Operational capabilities (policies and procedures)
Maintenance capabilities (policies and procedures)
Automation solution
Essential functions
Control functions
Safety functions
Complementary functions
IACS environment
Includes configured products (control systems and devices)
Role
Product supplier
Develops and supports
Develops and supports
Control system (as a combination of)
Software applications
Embedded devices
Network devices
Host devices
Independent of IACS environment
IEC

Figure 1 – Scope of service provider processes

In Figure 1, the Automation Solution is illustrated to contain essential functions that include safety functions, commonly implemented by a Safety Instrumented System (SIS), and complementary and control functions, commonly implemented by supporting applications, such as batch management, advanced control, historian, and security related applications. The dashed boxes identify organizational roles that perform the indicated actions.

NOTE 5 Automation Solutions typically have a single control system (product), but they are not restricted to do so. In general, the Automation Solution is the set of hardware and software, independent of product packaging, which is used to control a physical process (e.g. continuous or manufacturing) as defined by the asset owner.

NOTE 6 Service providers often provide generic architectures that can be adapted for integration into an Automation Solution. These generic architectures are often referred to as "reference architectures".

2 Normative references

There are no normative references in this document.

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- IEC Electropedia: available at https://www.electropedia.org/
- ISO Online browsing platform: available at https://www.iso.org/obp/

3.1.1
asset owner
role of an organization responsible for one or more IACSs

Note 1 to entry: The term "asset owner" is used in place of the generic term "end user" to provide differentiation.

Note 2 to entry: This definition includes the components that are part of the IACS.

Note 3 to entry: In the context of this document, asset owner also includes the operator of the IACS.

[SOURCE: IEC 62443-3-3:2013, 3.1.2, modified to be role-based.]

3.1.2
attack surface
physical and functional interfaces of a system that can be accessed and through which the system can be potentially exploited

Note 1 to entry: The size of the attack surface for a software interface is proportional to the number of methods and parameters defined for the interface. Simple interfaces, therefore, have smaller attack surfaces than complex interfaces.

Note 2 to entry: The size of the attack surface and the number of vulnerabilities are not necessarily related to each other.

3.1.3
Automation Solution
collection of control system and any complementary components that have been installed and configured to operate in an IACS

Note 1 to entry: Automation Solution is used as a proper noun in this document.

Note 2 to entry: The difference between the control system and the Automation Solution is that the control system is incorporated into the Automation Solution design (e.g. 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 Solution.

Note 3 to entry: The Automation Solution can be provided by multiple suppliers, including the product supplier of the control system and the product suppliers of complementary components.

Note 4 to entry: The Automation Solution does not include the processes and procedures used during integration, maintenance, and operation of the IACS.

Note 5 to entry: An Automation Solution, once integration into a given environment is complete, is ready for operation.

3.1.4
basic process control system
BPCS
system that responds to input signals from the process, its associated equipment, other programmable systems and/or an operator and generates output signals causing the process and its associated equipment to operate in the desired manner but does not perform any safety instrumented functions (SIF)

Note 1 to entry: Safety instrumented functions are specified in the IEC 61508 series.

Note 2 to entry: The term "process" in this definition can apply to a variety of industrial processes, including continuous processes and manufacturing processes.

3.1.5
component
entity belonging to an IACS that exhibits the characteristics of one or more of a host device, network device, software application, or embedded device

3.1.6
consultant
subcontractor that provides guidance, including expert advice, to the asset owner, integration or maintenance service provider, or product supplier

Note 1 to entry: A consultant can provide assistance for component or system countermeasures.

[SOURCE: ISO 15189:2022, 3.7, modified – subcontractor and roles added.]

3.1.7
control system
hardware and software components used in the design and implementation of an IACS

Note 1 to entry: As shown in Figure 1, control systems are composed of field devices, embedded control devices, network devices, and host devices (including workstations and servers).

Note 2 to entry: As shown in Figure 1, control systems are represented in the Automation Solution by a BPCS and an optional SIS.

[SOURCE: IEC 62443-3-3:2013, 3.1.16, modified to specify how it is used.]

3.1.8
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 can be considered essential.

[SOURCE: IEC 62443-3-3:2013, 3.1.22]

3.1.9
handover
act of turning an Automation Solution over to the asset owner

Note 1 to entry: Handover effectively transfers responsibility for operations and maintenance of an Automation Solution from the integration service provider to the asset owner and generally occurs after successful completion of system test, often referred to as Site Acceptance Test (SAT).

3.1.10
harden
process of improving the security of a system or component through a reduction of risk factors

Note 1 to entry: Hardening generally involves adapting and configuring the Automation Solution/components and related policies and procedures to meet the security needs of the asset owner's site.

3.1.11
industrial automation and control system
IACS
collection of personnel, hardware, software, procedures and policies involved in the operation of the industrial process and that can affect or influence its safe, secure and reliable operation

Note 1 to entry: The IACS can include components that are not installed at the asset owner's site.

Note 2 to entry: The definition of IACS is illustrated in Figure 1. Examples of IACSs include Distributed Control Systems (DCS) and Supervisory Control and Data Acquisition (SCADA) systems. This document also defines the proper noun "Automation Solution" to mean the specific instance of the control system product and possibly additional components that are designed into the IACS. The Automation Solution, therefore, differs from the control system since it represents a specific implementation (design and configuration) of the control system hardware and software components for a specific asset owner.

[SOURCE: IEC 62443-3-3:2013, 3.1.29, modified – Notes to entry added.]

3.1.12
integration service provider
service provider that provides integration activities for an Automation Solution including design, installation, configuration, testing, commissioning, and handover

Note 1 to entry: Integration service providers are often referred to as integrators or Main Automation Contractors (MAC).

3.1.13
maintenance service provider
service provider that provides support activities for an Automation Solution after handover

Note 1 to entry: Maintenance is often considered to be distinguished from operation (e.g. in common colloquial language, it is often assumed that an Automation Solution is either in operation or under maintenance). Maintenance service providers can perform support activities during operations, for example managing user accounts, security monitoring, and security assessments.

3.1.14
portable media
portable devices that contain data storage capabilities that can be used to physically copy data from one piece of equipment and transfer it to another

Note 1 to entry: Types of portable media include but are not limited to: CD/DVD/Blu-ray media, USB memory devices, smart phones, flash memory, solid state disks, hard drives, handhelds, and portable computers.

3.1.15
product
system, subsystem or component that is manufactured, developed or refined and that may be used in other products or integrated into an Automation Solution

Note 1 to entry: The processes required by the practices defined in this document apply iteratively to all levels of product design (for example, from the system level to the component level).

3.1.16
product supplier
manufacturer of hardware and/or software product

Note 1 to entry: Used in place of the generic word "vendor" to provide differentiation.

3.1.17
profile
named combination of options, chosen according to a specified framework, necessary to accomplish a particular function

Note 1 to entry: The options can be chosen from one or several documents or subdivisions of documents.

3.1.18
remote access
access to a control system through an external interface of the control system

Note 1 to entry: Examples of applications that support remote access include RDP, OPC, and Syslog.

Note 2 to entry: In general, remote access applications and the Automation Solution will reside in different security zones as determined by the asset owner. See IEC 62443-3-2 for the application of zones and conduits to the Automation Solution by the asset owner.

[SOURCE: IEC 62443-3-3:2013, 3.1.35, modified to specify access is through an external interface, and notes to entries added.]

3.1.19
safety instrumented system
system used to implement functional safety

Note 1 to entry: See the IEC 61508 series and the IEC 61511 series for more information on functional safety.

Note 2 to entry: Not all industry sectors use "safety instrumented system". This term is not restricted to any specific industry sector, and it is used generically to refer to systems that enforce functional safety. Other equivalent terms include "safety systems" and "safety related systems".

[SOURCE: IEC 62443-3-3:2013, 3.1.37, modified to be more general (implement functional safety), and notes to entries added.]

3.1.20
security compromise
violation of the security of a system such that an unauthorized (1) disclosure or modification of information or (2) denial of service could possibly have occurred

Note 1 to entry: A security compromise represents a breach of the security of a system or an infraction of its security policies. It is independent of impact or potential impact to the system.

3.1.21
security incident
security compromise that is of some significance to the asset owner or failed attempt to compromise the system whose result could have been of some significance to the asset owner

Note 1 to entry: The expression "of some significance" is relative to the environment in which the security compromise is detected. For example, the same compromise can be declared as a security incident in one environment and not in another. Triage activities are often used by asset owners to evaluate security compromises and identify those that are significant enough to be considered incidents.

Note 2 to entry: In some environments, failed attempts to compromise the system, such as failed login attempts, are considered significant enough to be classified as security incidents.

3.1.22
security patch
software update that is relevant to the security of a software component

Note 1 to entry: For the purpose of this definition, firmware is considered software.

Note 2 to entry: Software patches can address known or potential vulnerabilities, or simply improve the security of the software component, including its reliable operation.