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

EESTI STANDARDIMIS- JA AKREDITEERIMISKESKUS
ESTONIAN CENTRE FOR STANDARDISATION AND ACCREDITATION

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN IEC 62443-2-4:2024 sisaldab Euroopa standardi EN IEC 62443-2-4:2024 ingliskeelset teksti.	This Estonian standard EVS-EN IEC 62443-2-4:2024 consists of the English text of the European standard EN IEC 62443-2-4:2024.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas.	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation and Accreditation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 26.01.2024.	Date of Availability of the European standard is 26.01.2024.
Standard on kättesaadav Eesti Standardimis-ja Akrediteerimiskeskusest.	The standard is available from the Estonian Centre for Standardisation and Accreditation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 25.040.40, 35.100.05

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

IEC 62443-2-4:2023-12(en-fr)

IEC Secretariat
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, …). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch
Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 300 terminological entries in English and French, with equivalent terms in 19 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC - webstore.iec.ch/advsearchform
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, …). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch
Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org
Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 300 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 19 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

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

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.

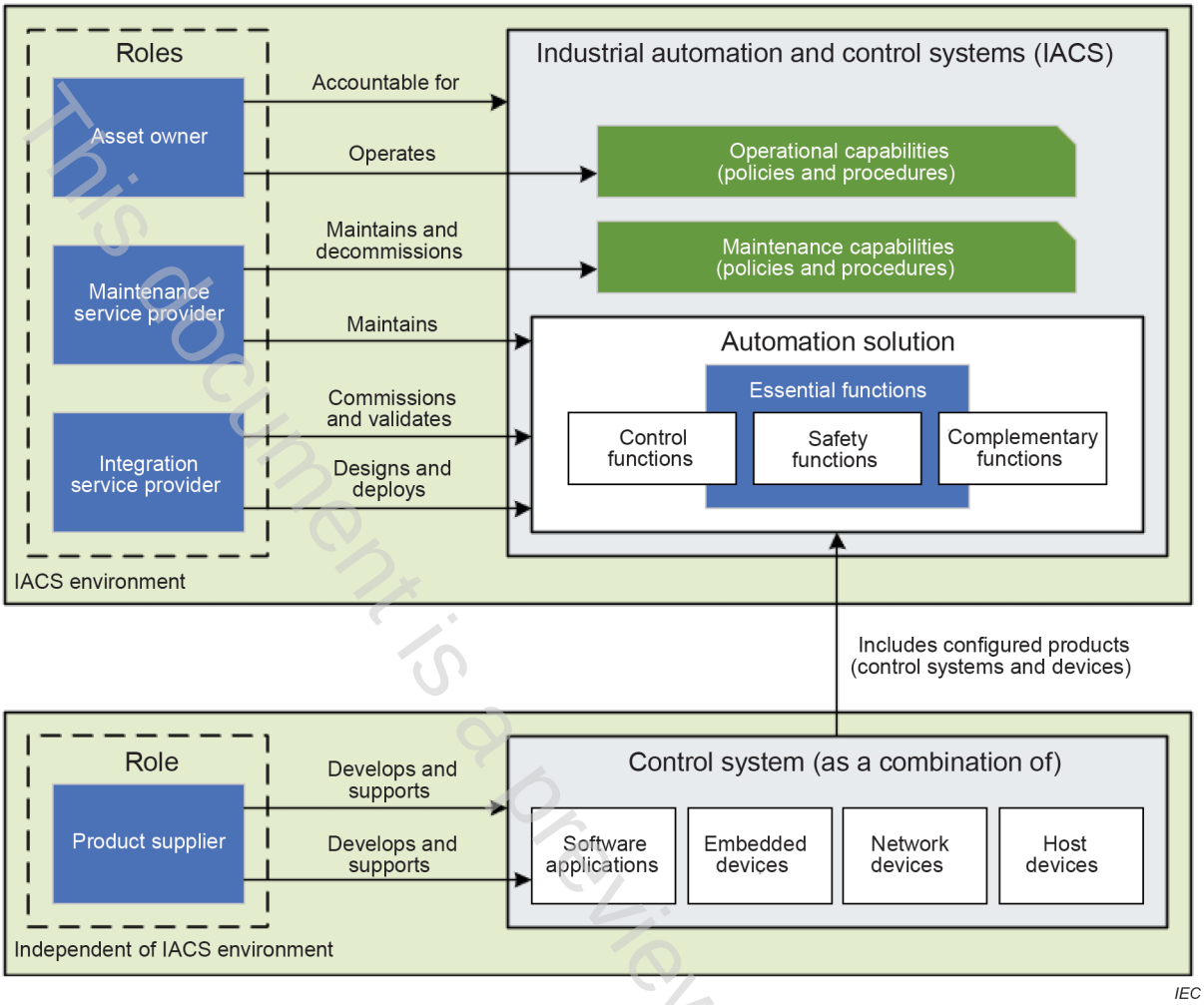

Figure 1 – Scope of service provider processes

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.