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

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN IEC 62443-2-4:2019 sisaldab Euroopa standardi EN IEC 62443-2-4:2019 ingliskeelset teksti.	This Estonian standard EVS-EN IEC 62443-2-4:2019 consists of the English text of the European standard EN IEC 62443-2-4:2019.
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.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 19.04.2019.	Date of Availability of the European standard is 19.04.2019.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

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

April 2019

ICS 25.040.40; 35.100.05

English Version

Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers (IEC 62443-2-4:2015)

Sécurité des automatismes industriels et des systèmes de commande - Partie 2-4: Exigences de programme de sécurité pour les fournisseurs de service IACS (IEC 62443-2-4:2015)

IT-Sicherheit für industrielle Automatisierungssysteme - Teil 2-4: Anforderungen an das IT-Sicherheitsprogramm von Dienstleistern für industrielle Automatisierungssysteme (IEC 62443-2-4:2015)

This European Standard was approved by CENELEC on 2019-04-03. 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, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey 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

This document (EN IEC 62443-2-4:2019) consists of the text of IEC 62443-2-4:2015 prepared by IEC/TC 65 "Industrial-process measurement, control and automation".

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) 2020-04-03
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2022-04-03

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.

Endorsement notice

The text of the International Standard IEC 62443-2-4:2015 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 standards indicated:

IEC 61508 (series)	NOTE	Harmonized as EN 61508 (series)
IEC 61511 (series)	NOTE	Harmonized as EN 61511 (series)
IEC 62264-1:2013	NOTE	Harmonized as EN 62264-1:2013 (not modified)
IEC 62443-3-3:2013	NOTE	Harmonized as EN IEC 62443-3-3:2019 (not modified)
IEC 62443-4-1	NOTE	Harmonized as EN IEC 62443-4-1
IEC 62443-4-2	NOTE	Harmonized as EN IEC 62443-4-2

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

International Standard IEC 62443-2-4 has been prepared by IEC technical committee 65: Industrial-process measurement, control and automation.

This publication contains an attached file in the form of an Excel 97-2003 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.

The text of this standard is based on the following documents:

CDV	Report on voting
65/545/CDV	65/561A/RVC

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

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

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 publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

The contents of the corrigendum of August 2015 have been included in this copy.

IMPORTANT – The 'colour inside' logo on the cover page of this publication 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.

INTRODUCTION

This standard is the part of the IEC 62443 series that contains security requirements for providers of integration and maintenance services for Industrial Automation and Control Systems (IACS). It has been developed by IEC Technical Committee 65 in collaboration with the International Instrumentation Users Association, referred to as the WIB from its original and now obsolete Dutch name, and ISA 99 committee members.

Figure 1 illustrates the relationship of the different parts of IEC 62443 being developed. Those that are normatively referenced are included in the list of normative references in Clause 2, and those that are referenced for informational purposes or that are in development are listed in the Bibliography.

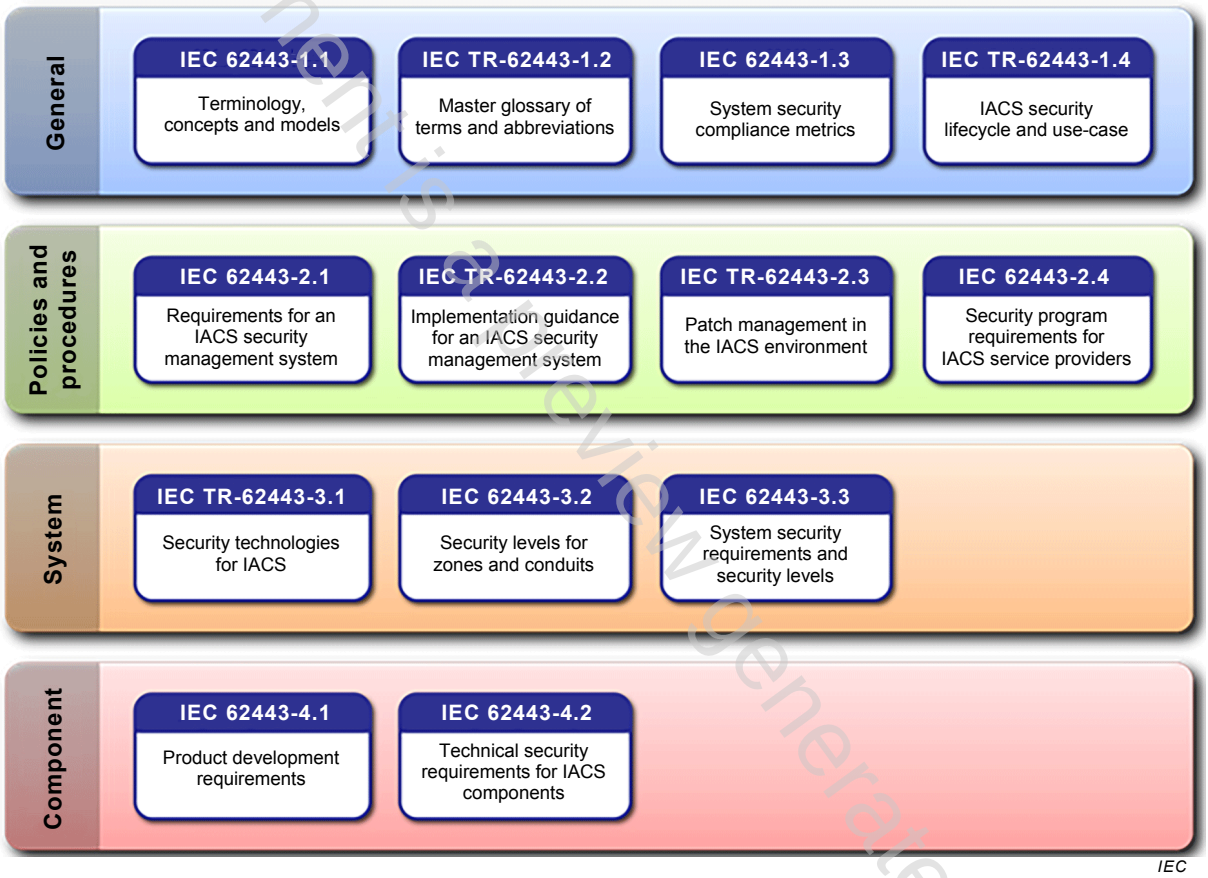

Figure 1 – Parts of the IEC 62443 Series

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

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

1 Scope

This part of IEC 62443-2-4 specifies requirements for security capabilities for IACS service providers that they can offer to the asset owner during integration and maintenance activities of an Automation Solution.

NOTE 1 The term “Automation Solution” is used as a proper noun (and therefore capitalized) in this part of IEC 62443 to prevent confusion with other uses of this term.

Collectively, the security capabilities offered by an IACS service provider are referred to as its Security Program. 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 2 illustrates how the integration and maintenance capabilities relate to the IACS and the control system product that is integrated into the Automation Solution. Some of these capabilities reference security measures defined in IEC 62443-3-3 that the service provider must ensure are supported in the Automation Solution (either included in the control system product or separately added to the Automation Solution).

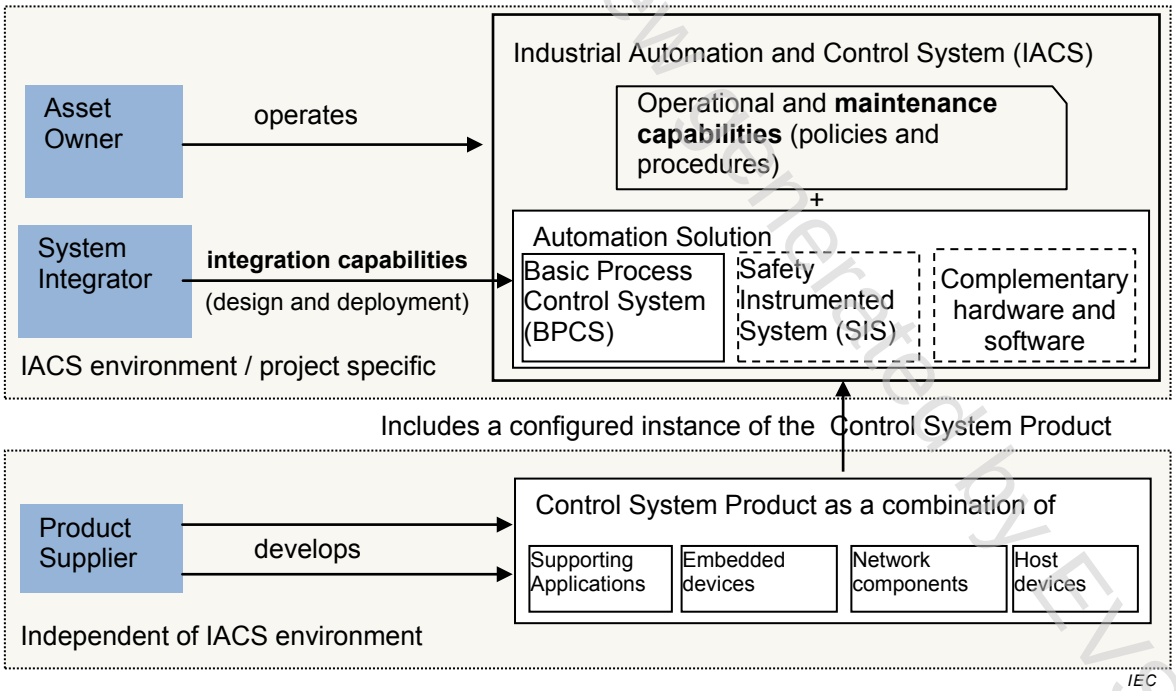

Figure 2 – Scope of service provider capabilities

In Figure 2, the Automation Solution is illustrated to contain a Basic Process Control System (BPCS), optional Safety Instrumented System (SIS), and optional supporting applications, such as advanced control. The dashed boxes indicate that these components are “optional”.

NOTE 3 The term “process” in BPCS may apply to a variety of industrial processes, including continuous processes and manufacturing processes.

NOTE 4 Clause 4.1.4 describes profiles and how they can be used by industry groups and other organizations to adapt this International Standard to their specific environments, including environments not based on an IACS.

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, that is used to control a physical process (e.g. continuous or manufacturing) as defined by the asset owner.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

“None”

3 Terms, definitions, abbreviated terms and acronyms

3.1 Terms and definitions

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

3.1.1
asset owner
individual or organization responsible for one or more IACSs

Note 1 to entry: Used in place of the generic word 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 standard, asset owner also includes the operator of the IACS.

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
control system and any complementary hardware and software 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 part of IEC 62443.

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 may be comprised of components from multiple suppliers, including the product supplier of the control system.