EESTI STANDARD EVS-EN IEC 62443-2-1:2024

Security for industrial automation and control systems - Part 2-1: Security program requirements for IACS asset owners

EESTI STANDARDIMIS- JA AKREDITEERIMISKESKUS
ESTONIAN CENTRE FOR STANDARDISATION AND ACCREDITATION

EESTI STANDARDI EESSÕNA	NATIONAL FOREWORD
See Eesti standard EVS-EN IEC 62443-2-1:2024 sisaldab Euroopa standardi EN IEC 62443-2-1:2024 ingliskeelset teksti.	This Estonian standard EVS-EN IEC 62443-2-1:2024 consists of the English text of the European standard EN IEC 62443-2-1:2024.
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 20.09.2024.	Date of Availability of the European standard is 20.09.2024.
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 62443-2-1

September 2024

ICS 25.040.40; 35.100.05

English Version

Security for industrial automation and control systems - Part 2-1: Security program requirements for IACS asset owners (IEC 62443-2-1:2024)

Sécurité des systèmes d'automatisation et de commande industrielles - Partie 2-1: Exigences de programme de sécurité pour les propriétaires d'actif IACS (IEC 62443-2-1:2024)

IT-Sicherheit für industrielle Automatisierungssysteme - Teil 2-1: Anforderungen an ein IT-Sicherheitsprogramm für IACS-Betreiber (IEC 62443-2-1:2024)

This European Standard was approved by CENELEC on 2024-09-11. 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.

CENELEC

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 65/1044/FDIS, future edition 2 of IEC 62443-2-1, prepared by TC 65 "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 62443-2-1:2024.

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) 2025-06-11
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2027-09-11

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 62443-2-1:2024 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 62443-3-2:2020	NOTE Approved as EN IEC 62443-3-2:2020 (not modified)
IEC 62443-2-4:2023	NOTE Approved as EN IEC 62443-2-4:2024 (not modified)
IEC 62443-3-3:2013	NOTE Approved as EN IEC 62443-3-3:2019 (not modified)
IEC 62443-4-2:2019	NOTE Approved as EN IEC 62443-4-2:2019 (not modified)
ISO/IEC 27000:2018	NOTE Approved as EN ISO/IEC 27000:2020 (not modified)
IEC 62443-4-1:2018	NOTE Approved as EN IEC 62443-4-1:2018 (not modified)
ISO/IEC 17000:2020	NOTE Approved as EN ISO/IEC 17000:2020 (not modified)
ISO/IEC 27002:2022	NOTE Approved as EN ISO/IEC 27002:2022 (not modified)
IEC 62591:2016	NOTE Approved as EN 62591:2016 (not modified)
IEC 62734:2014	NOTE Approved as EN 62734:2015 (not modified)

IEC 62443-2-1

Edition 2.0 2024-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

HORIZONTAL PUBLICATION
PUBLICATION HORIZONTALE

Security for industrial automation and control systems – Part 2-1: Security program requirements for IACS asset owners

Sécurité des systèmes d’automatisation et de commande industrielles – Partie 2-1: Exigences de programme de sécurité pour les propriétaires d’actif IACS

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

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

IEC 62443-2-1

Edition 2.0 2024-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Security for industrial automation and control systems – Part 2-1: Security program requirements for IACS asset owners

Sécurité des systèmes d'automatisation et de commande industrielles – Partie 2-1: Exigences de programme de sécurité pour les propriétaires d'actif IACS

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 25.040.40, 35.100.05

ISBN 978-2-8322-9459-8

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

FOREWORD ... 6
INTRODUCTION ... 8
1 Scope ... 10
2 Normative references ... 11
3 Terms, definitions, abbreviated terms and conventions ... 11
3.1 Terms and definitions ... 11
3.2 Abbreviated terms and acronyms ... 15
3.3 Conventions ... 16
4 Concepts ... 17
4.1 Use of this document ... 17
4.1.1 Applicable roles ... 17
4.1.2 Use of this document by asset owners ... 17
4.1.3 Use of this document by service providers and product suppliers ... 19
4.2 Maturity level (ML) definitions ... 20
4.3 Security levels (SLs) ... 21
4.4 Requirements definitions ... 21
4.4.1 Requirements organization ... 21
4.4.2 Requirements cross-references ... 22
4.4.3 Requirement conventions ... 22
5 Conformance and assessment ... 22
5.1 Overview ... 22
5.2 Conformity evidence ... 23
5.3 Requirements evaluation and profiles ... 24
5.3.1 Overview ... 24
5.3.2 Evaluation of risk to requirements ... 24
5.3.3 Profiles ... 24
5.3.4 Conformity assessment for the asset owner role ... 25
6 SPE 1 – Organizational security measures ... 25
6.1 Purpose ... 25
6.2 ORG 1 – Security related organization and policies ... 25
6.2.1 ORG 1.1: Information security management system (ISMS) ... 25
6.2.2 ORG 1.2: Background checks ... 26
6.2.3 ORG 1.3: Security roles and responsibilities ... 26
6.2.4 ORG 1.4: Security awareness training ... 27
6.2.5 ORG 1.5: Security responsibilities training ... 27
6.2.6 ORG 1.6: Supply chain security ... 28
6.3 ORG 2 – Security assessments and reviews ... 28
6.3.1 ORG 2.1: Security risk mitigation ... 28
6.3.2 ORG 2.2: Processes for discovery of security anomalies ... 29
6.3.3 ORG 2.3: Secure development and support ... 30
6.3.4 ORG 2.4: SP reviews ... 30
6.4 ORG 3 – Security of physical access ... 30
6.4.1 ORG 3.1: Physical access control ... 30
7 SPE 2 – Configuration management ... 31
7.1 Purpose ... 31

7.2 CM 1 – Inventory management of IACS hardware/software components and network communications 31
7.2.1 CM 1.1: Asset inventory baseline 31
7.2.2 CM 1.2: Infrastructure drawings/documentation 32
7.2.3 CM 1.3: Configuration settings 32
7.2.4 CM 1.4: Change control 33
8 SPE 3 – Network and communications security 33
8.1 Purpose 33
8.2 NET 1 – System segmentation 33
8.2.1 NET 1.1: Segmentation from non-IACS zones 33
8.2.2 NET 1.2: Documentation of zones and network zone interconnections 34
8.2.3 NET 1.3: Network segmentation from safety systems 34
8.2.4 NET 1.4: Network autonomy 35
8.2.5 NET 1.5: Network disconnection from external networks 35
8.2.6 NET 1.6: Internal network access control 35
8.2.7 NET 1.7: Network accessible services 36
8.2.8 NET 1.8: User messaging 36
8.2.9 NET 1.9: Network time distribution 36
8.3 NET 2 – Secure wireless access 37
8.3.1 NET 2.1: Wireless protocols 37
8.3.2 NET 2.2: Wireless network segmentation 37
8.3.3 NET 2.3: Wireless properties and addresses 38
8.4 NET 3 – Secure remote access 38
8.4.1 NET 3.1: Remote access applications 38
8.4.2 NET 3.2: Remote access connections 39
8.4.3 NET 3.3: Remote access termination 39
9 SPE 4 – Component security 40
9.1 Purpose 40
9.2 COMP 1 – Components and portable media 40
9.2.1 COMP 1.1: Component hardening 40
9.2.2 COMP 1.2: Dedicated portable media 41
9.3 COMP 2 – Malware protection 41
9.3.1 COMP 2.1: Malware free 41
9.3.2 COMP 2.2: Malware protection 42
9.3.3 COMP 2.3: Malware protection software validation and installation 42
9.4 COMP 3 – Patch management 43
9.4.1 COMP 3.1: Security patch authenticity/integrity 43
9.4.2 COMP 3.2: Security patch validation and installation 43
9.4.3 COMP 3.3: Security patch status 43
9.4.4 COMP 3.4: Security patching retention of security 44
9.4.5 COMP 3.5: Security patch mitigation 44
10 SPE 5 – Protection of data 44
10.1 Purpose 44
10.2 DATA 1 – Protection of data 45
10.2.1 DATA 1.1: Data classification 45
10.2.2 DATA 1.2: Data confidentiality 45
10.2.3 DATA 1.3: Safety system configuration mode 46
10.2.4 DATA 1.4: Data retention policy 46
10.2.5 DATA 1.5: Cryptographic mechanisms 47

10.2.6 DATA 1.6: Key management 47
10.2.7 DATA 1.7: Data Integrity 47
11 SPE 6 – User access control 48
11.1 Purpose 48
11.2 USER 1 – Identification and authentication 48
11.2.1 USER 1.1: User identity assignment 48
11.2.2 USER 1.2: User identity removal....49
11.2.3 USER 1.3: User identity persistence 49
11.2.4 USER 1.4: Access rights assignment 50
11.2.5 USER 1.5: Least privilege 50
11.2.6 USER 1.6: Software service authentication 50
11.2.7 USER 1.7: Software services interactive login rights 51
11.2.8 USER 1.8: Human user authentication 51
11.2.9 USER 1.9: Multifactor authentication (MFA) 51
11.2.10 USER 1.10: Mutual authentication 52
11.2.11 USER 1.11: Password protection 52
11.2.12 USER 1.12: Shared and disclosed/compromised passwords 53
11.2.13 USER 1.13: User login display information....53
11.2.14 USER 1.14: User login failure displays 53
11.2.15 USER 1.15: Consecutive login failures....54
11.2.16 USER 1.16: Session integrity....54
11.2.17 USER 1.17: Concurrent sessions 54
11.2.18 USER 1.18: Screen lock 55
11.2.19 USER 1.19: Component authentication 55
11.3 USER 2 – Authorization and access control 55
11.3.1 USER 2.1: Authorization 55
11.3.2 USER 2.2: Separation of duties 56
11.3.3 USER 2.3: Multiple approvals 56
11.3.4 USER 2.4: Manual elevation of privileges 57
12 SPE 7 – Event and incident management 57
12.1 Purpose 57
12.2 EVENT 1 – Event and incident management 57
12.2.1 EVENT 1.1: Event detection 57
12.2.2 EVENT 1.2: Event reporting....58
12.2.3 EVENT 1.3: Event reporting interfaces....58
12.2.4 EVENT 1.4: Logging 59
12.2.5 EVENT 1.5: Log entries 59
12.2.6 EVENT 1.6: Log access 59
12.2.7 EVENT 1.7: Event analysis 60
12.2.8 EVENT 1.8: Incident handling and response 60
12.2.9 EVENT 1.9: Vulnerability handling 60
13 SPE 8 – System integrity and availability....61
13.1 Purpose 61
13.2 AVAIL 1 – System availability and intended functionality....61
13.2.1 AVAIL 1.1: Continuity management 61
13.2.2 AVAIL 1.2: Resource availability management 62
13.2.3 AVAIL 1.3: Failure-state....62
13.3 AVAIL 2 – Backup/restore/archive....62
13.3.1 AVAIL 2.1: Backup....62

13.3.2 AVAIL 2.2: Backup non-interference 63
13.3.3 AVAIL 2.3: Backup verification 63
13.3.4 AVAIL 2.4: Backup media 63
13.3.5 AVAIL 2.5: Backup restoration 64
Annex A (informative) Cross-references to other standards 65
A.1 Requirements relationship to IEC 62443-2-4 65
A.2 Requirements relationship to IEC 62443-3-3 68
A.3 Requirements relationship to IEC 62443-4-2 70
A.4 Requirements relationship to ISO/IEC 27001:2013 73
A.5 Requirements relationship to the NIST CSF 77
Annex B (informative) Establishing and maintaining an IACS SP 81
B.1 General 81
B.2 Managing cybersecurity risk 82
B.2.1 Understanding cybersecurity risk 82
B.2.2 Impacts of cybersecurity compromises 82
B.2.3 Risk ranking 82
B.2.4 Cybersecurity attack exposure versus likelihood 83
B.3 Elements of a cybersecurity risk assessment/management process 84
B.4 Elements of a cybersecurity risk assessment/management process 85
Annex C (informative) Evaluating MLs 87
C.1 Approach to evaluating MLs 87
C.2 Examples of how to evaluate MLs 88
Bibliography 89

Figure 1 – Roles and responsibilities in the IEC 62443 series 11
Figure B.1 – Example of process flow for cybersecurity risk management 85
Figure B.2 – Levels of protection an asset requires 86

Table 1 – ML levels and descriptions 20
Table 2 – Typical conformity evidence types 23
Table A.1 – IEC 62443-2-4 cross-references 65
Table A.2 – Cross-reference of IEC 62443-2-1 to IEC 62443-2-4 66
Table A.3 – IEC 62443-3-3 cross-references 68
Table A.4 – Cross-reference of IEC 62443-2-1 to IEC 62443-3-3 69
Table A.5 – IEC 62443-4-2 cross-references 70
Table A.6 – Cross-reference of IEC 62443-2-1 to IEC 62443-4-2 72
Table A.7 – ISO/IEC 27001:2013 cross-references 73
Table A.8 – Cross-reference of IEC 62443-2-1 to ISO/IEC 27001:2013 75
Table A.9 – NIST CSF cross-references 77
Table A.10 – Cross-reference of IEC 62443-2-1 to NIST CSF 79
Table B.1 – Example risk levels 83

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 2-1: Security program requirements for IACS asset owners

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.

IEC 62443-2-1 has been prepared by IEC technical committee 65: Industrial process measurement, control and automation, in collaboration with the liaison ISA99: ISA committee on Security for industrial automation and control systems. It is an International Standard.

This second edition cancels and replaces the first edition published in 2010. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) revised requirement structure into SP elements (SPEs),

b) revised requirements to eliminate duplication of an information security management system (ISMS), and

c) defined a maturity model for evaluating requirements.

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

Draft	Report on voting
65/1044/FDIS	65/1053/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.

INTRODUCTION

This document is the part of the IEC 62443 series that contains security requirements for industrial automation and control system (IACS) asset owners. In the context of this document, asset owner also includes the operator of the IACS. Its requirements focus on cybersecurity and allow security capabilities that meet them to be provided as a combination of technical, physical, process and compensating security measures.

Cybersecurity is an increasingly important topic in modern organizations. The term cybersecurity is generally used to describe the set of security measures or practices taken to protect a computer or computer system against unauthorized access or attack. In IACS, the most significant concerns include unwanted access or attacks resulting in the IACS not performing the correct functions in the required timeframe.

A very common engineering approach when faced with a challenging problem is to break the problem into smaller pieces and address each piece in a disciplined manner. This approach is a sound one for addressing cybersecurity risks with IACS. However, a frequent mistake is to deal with cybersecurity one system at a time. Cybersecurity is a much larger challenge that should address all IACS components as well as the policies, procedures, practices and personnel that surround and utilize those IACS. Implementing such a wide-ranging management system can require a cultural change within the organization.

Addressing cybersecurity on an organization-wide basis can seem like a daunting task. There is no simple cookbook for security, nor is there a one-size-fits-all set of security practices. Absolute security can be achievable but is probably undesirable because of the loss of functionality that would be necessary to achieve this near perfect state. Security is a balance of risk versus cost.

Each situation will be different. In some situations, the risk can be related to health, safety and environmental (HSE) factors rather than purely economic impact. The risk can have an unrecoverable consequence rather than a temporary financial setback. Therefore, a predetermined set of mandatory security practices can either be overly restrictive and likely quite costly to implement or be insufficient to address the risk.

This document supports the need to address cybersecurity for an IACS in operation by providing requirements for establishing, implementing, maintaining and continually improving an IACS security program (SP). These requirements, when implemented conscientiously, provide security capabilities whose purpose is to reduce IACS security risks to a tolerable level. These requirements are written to be implementation independent, allowing asset owners to select approaches most suitable to their needs. IEC 62443-3-2 [1][1] describes the methodology for addressing cybersecurity risks in an IACS system design and that assists in the identification of risks and the selection of appropriate security requirements and associated capabilities for an IACS SP.

Commercial-off-the-shelf (COTS) products are often not ruggedized or rigorously engineered enough for IACS environments, where they can introduce additional vulnerabilities and threats to the IACS.

[1] Numbers in square brackets refer to the Bibliography.

When COTS technologies are used in an IACS, they are often configured to meet IACS specific functional needs and operational constraints. For example, security event handling in COTS products may be configured differently for IACS applications than they are for traditional information technology (IT) applications. Typical COTS equipment is designed for environments where the primary objective is the protection of information. In an IACS environment, the primary objectives are the protection of the HSE of the facility and the minimization of the operational and business impact on facility operation. COTS technologies can be applied to IACS applications, but the risks associated with using these technologies need to be understood by the asset owner.

Some organizations can attempt to use pre-existing IT and business cybersecurity solutions to address security for IACS without understanding the consequences. While many of these solutions can be applied to IACS, it is important to apply them correctly to eliminate inadvertent and undesired consequences. For example, in an IACS, availability may have a higher priority than confidentiality, as opposed to typical IT applications.

Asset owners may wish to apply their IACS SP across the organization to address the organization needs and objectives, security requirements, business and work processes, as well as the organization size and structure. All of these influencing factors are dynamic and will likely change over time. Thus, the adoption of an IACS SP is a strategic decision for the organization.

The effectiveness of an IACS SP is often enhanced through coordination or integration with the organization's processes and overall information security management system (ISMS). For example, security can be added to the organization supply chain processes to require security in the design of processes, systems and controls. It is also expected that IACS SP will be scaled in accordance with the needs of the IACS and the organization.

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 2-1: Security program requirements for IACS asset owners

1 Scope

This part of IEC 62443 specifies asset owner security program (SP) policy and procedure requirements for an industrial automation and control system (IACS) in operation. This document uses the broad definition and scope of what constitutes an IACS as described in IEC TS 62443-1-1. In the context of this document, asset owner also includes the operator of the IACS.

This document recognizes that the lifespan of an IACS can exceed twenty years, and that many legacy systems contain hardware and software that are no longer supported. Therefore, the SP for most legacy systems addresses only a subset of the requirements defined in this document. For example, if IACS or component software is no longer supported, security patching requirements cannot be met. Similarly, backup software for many older systems is not available for all components of the IACS. This document does not specify that an IACS has these technical requirements. This document states that the asset owner needs to have policies and procedures around these types of requirements. In the case where an asset owner has legacy systems that do not have the native technical capabilities, compensating security measures can be part of the policies and procedures specified in this document.

This document also recognizes that not all requirements specified in this document apply to all IACSs. For example, requirements associated with certain technology (such as wireless) or functions (such as remote access) will not apply to IACSs that do not include these technologies or functions. Similarly, not all malware protection requirements apply to systems for which malware protection software is not available for any of their devices. Therefore, this document states that the asset owner needs to identify the IACS security requirements that are applicable to its IACSs in their specific operating environments.

The elements of an IACS SP described in this document define required security capabilities that apply to the secure operation of an IACS. Although the asset owner is ultimately accountable for the secure operation of an IACS, implementation of these security capabilities often includes support from its service providers and product suppliers. For this reason, this document provides guidance for an asset owner when stating security requirements for their service providers and product suppliers, referencing other parts of the IEC 62443 series.

Figure 1 illustrates the roles and responsibilities 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. The Automation Solution is a technical solution implementing the control/safety and complementary functions necessary for the IACS. It is composed of hardware and software components that have been installed and configured to operate in the IACS. The IACS is a combination of the Automation Solution and the organizational measures necessary for its design, deployment, operation and maintenance.

Some of these capabilities rely on the appropriate application of integration maintenance capabilities defined in IEC 62443-2-4 [2] and technical security capabilities defined in IEC 62443-3-3 [3] and IEC 62443-4-2 [4].

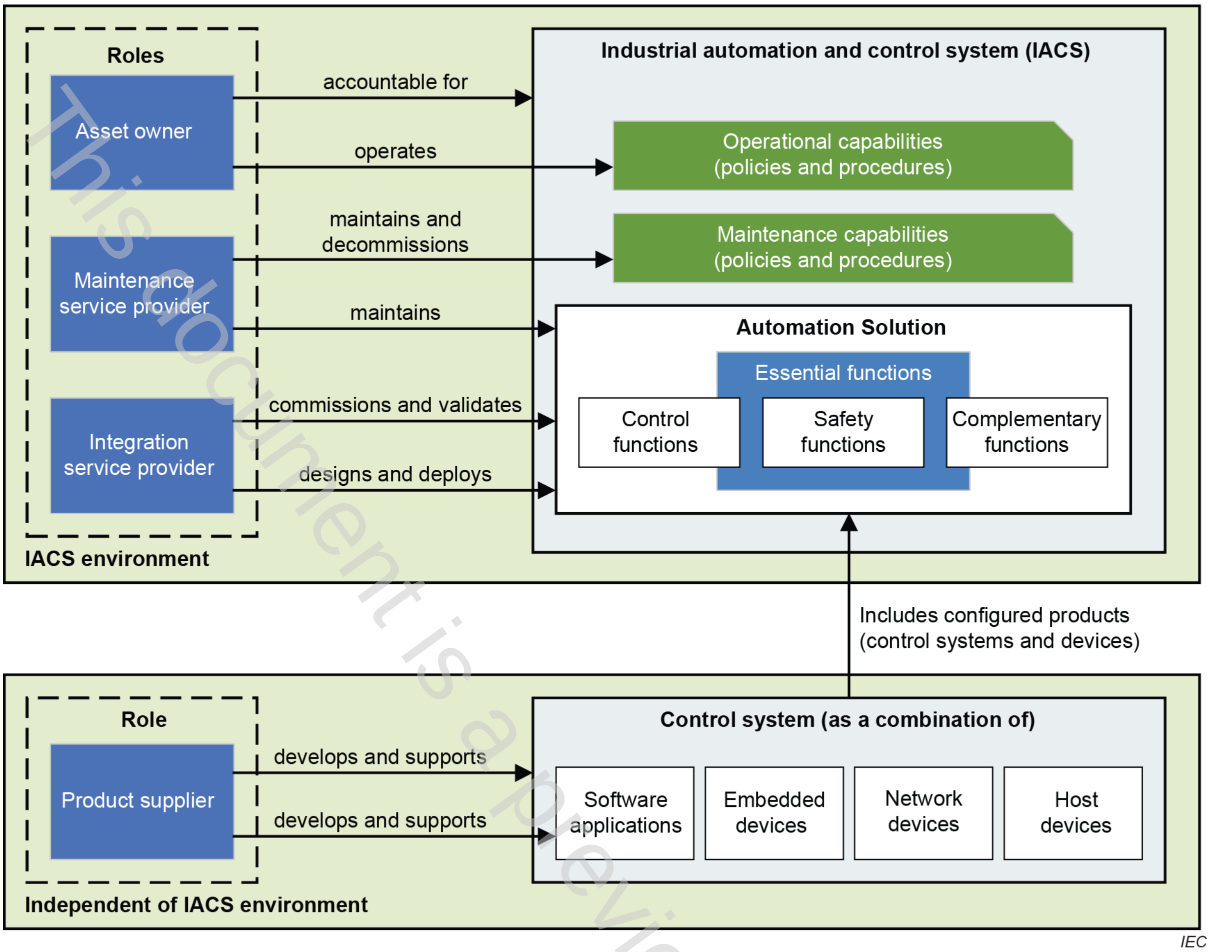
Roles
Asset owner
Maintenance service provider
Integration service provider
accountable for
operates
maintains and decommissions
maintains
commissions and validates
designs and deploys
Industrial automation and control system (IACS)
Operational capabilities (policies and procedures)
Maintenance capabilities (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 – Roles and responsibilities in the IEC 62443 series

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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.

IEC TS 62443-1-1:2009, *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*

3 Terms, definitions, abbreviated terms and conventions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC TS 62443-1-1 and the following apply.

ISO and IEC maintain terminological 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