BS EN IEC 62443-2-4:2024

BSI Standards Publication

Security for industrial automation and control systems

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

Documents
Document Sharing Hub

Full document details: BS EN IEC 62443-2-4:2024

National foreword

This British Standard is the UK implementation of EN IEC 62443-2-4:2024. It is identical to IEC 62443-2-4:2023. It supersedes BS EN IEC 62443-2-4:2019+A1:2019, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee GEL/65, Measurement and control.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2024
Published by BSI Standards Limited 2024

ISBN 978 0 539 15511 2

ICS 25.040.40; 35.100.05

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 29 February 2024.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS EN IEC 62443-2-4:2024

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

© 2024 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

Ref. No. EN IEC 62443-2-4:2024 E

Documents
Document Sharing Hub

Full document details: BS EN IEC 62443-2-4:2024

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)

Documents
Document Sharing Hub

Full document details: BS EN IEC 62443-2-4:2024

CONTENTS

FOREWORD 3
1 Scope 5
2 Normative references 6
3 Terms, definitions and abbreviated terms 7
3.1 Terms and definitions 7
3.2 Abbreviated terms 11
4 Concepts 13
4.1 Use of this document 13
4.1.1 Use of this document by service providers 13
4.1.2 Use of this document by asset owners 14
4.1.3 Use of this document during negotiations between asset owners and IACS service providers 15
4.1.4 Profiles 15
4.1.5 Integration service providers 15
4.1.6 Maintenance service providers 16
4.2 Maturity model 17
5 Requirements overview 18
5.1 Contents 18
5.2 Sorting and filtering 19
5.3 IEC 62264-1 hierarchy model 19
5.4 Requirements table columns 19
5.5 Column definitions 19
5.5.1 Req ID column 19
5.5.2 BR/RE column 20
5.5.3 Functional area column 20
5.5.4 Topic column 21
5.5.5 Subtopic column 22
5.5.6 Documentation column 24
5.5.7 Requirement description column 24
5.5.8 Rationale column 25
Annex A (normative) Security requirements 26
Bibliography 91

Figure 1 – Scope of service provider processes 6

Table 1 – Maturity levels 18
Table 2 – Columns 19
Table 3 – Functional area column values 21
Table 4 – Architecture Functional Area Summary Levels 21
Table 5 – Topic column values 22
Table 6 – Subtopic column values 23
Table A.1 – Security program requirements 26

Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2024

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.

Documents
Document Sharing Hub

Full document details: BS EN IEC 62443-2-4:2024

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.

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 62443-2-4:2024

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.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2024

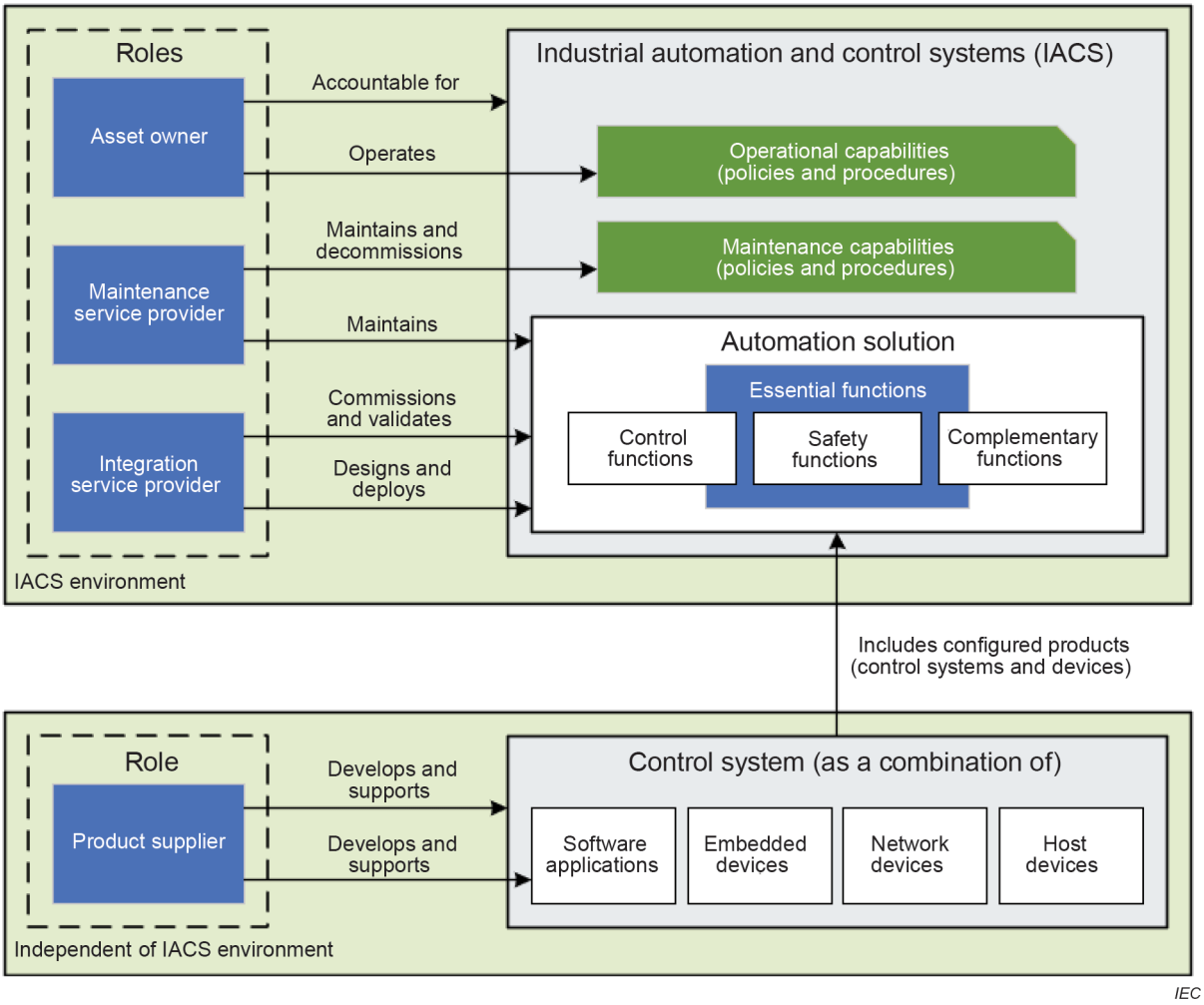

Figure 1 – Scope of service provider processes

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.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2024

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.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2024

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).

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 62443-2-4:2024

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.

AVA Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2024

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.

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 62443-2-4:2024

3.1.23
security program
portfolio of security services, including integration services and maintenance services, and their associated policies, procedures, and products that are applicable to the IACS

Note 1 to entry: The security program for IACS service providers refers to the policies and procedures defined by them to address security concerns of the IACS.

3.1.24
service provider
role of an organization (internal or external organization, manufacturer, etc.) that provides a specific support service and associated supplies in accordance with an agreement with the asset owner

Note 1 to entry: This term is used in place of the generic word "vendor" to provide differentiation.

[SOURCE: IEC 62443-3-3:2013, 3.1.39, modified to be role-based.]

3.1.25
subcontractor
service provider under contract to the integration or maintenance service provider or to another subcontractor that is directly or indirectly under contract to the integration or maintenance service provider

3.1.26
system
interacting, interrelated, or interdependent elements forming a complex whole

Note 1 to entry: A system can possibly be packaged as a product.

Note 2 to entry: In practice, the interpretation of the meaning of "system" is frequently clarified by the use of an adjective, such as control system. In the context of a control system, the elements are largely hardware and software elements.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.123, modified – Notes to entry added.]

3.1.27
verify
check that the specified requirement was met

3.1.28
vulnerability
flaw or weakness in the design, implementation, or operation and management of a component that can be exploited to cause a security compromise

Note 1 to entry: Security policies typically include policies to protect confidentiality, integrity, and availability of system assets.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.135, modified – generalized to cause a security compromise.]

3.2 Abbreviated terms

ABAC	Attribute-Based Access Control
AES_GCM	Advanced Encryption Standard Galois/Counter Mode
ANSI	American National Standards Institute
BPCS	Basic Process Control System
BR	Base Requirement
CA	Certificate Authority

Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2024

CD	Compact Disk
CEF	Common Event Format
CMMI	Capability Maturity Model Integration
DCS	Distributed Control System
DES	Data Encryption Standard
DVD	Digital Video Disk, Digital Versatile Disk
EICAR	European Institute of Computer Anti-virus Research
EWS	Engineering Workstation
FAT	Factory Acceptance Test
IACS	Industrial Automation and Control System
ID	Identifier
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevent System
ISA	International Society of Automation
LDAP	Lightweight Directory Access Protocol
MAC	Main Automation Contractor
MIB	Management Information Base
MoC	Management of Change
NAMUR	User Association of Automation Technology in Process Industries
NDA	Non-Disclosure Agreement
NIDS	Network Intrusion and Detection System
OPC	Open Platform Communications
PAS	Publicly Available Specification
PBAC	Policy-Based Access Control
PtW	Permit to Work
RBAC	Role-Based Access Control
RE	Requirement Enhancement
RDP	Remote Desktop Protocol
RFC	Request For Comment
RFQ	Request For Quote
SAT	Site Acceptance Test
SCADA	Supervisory Control And Data Acquisition
SIEM	Security Information and Event Management
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SNMP	Simple Network Management Protocol
SOW	Statement Of Work
SSID	Service Set Identifier
SP	Security Program
TCP	Transmission Control Protocol
TR	Technical Report

Documents
Document Sharing Hub

Full document details: BS EN IEC 62443-2-4:2024

UDP	User Datagram Protocol
USB	Universal Serial Bus
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy

4 Concepts

4.1 Use of this document

4.1.1 Use of this document by service providers

"Service provider" and "asset owner" are terms that represent roles of an organization. While they can be in the same organization, they are typically in separate organizations, with the service provider's organization under contract/agreement to the asset owner's organization.

This document defines a single set of requirements for security-related processes to be supported by security programs of both integration and maintenance service providers (see 4.1.5 and 4.1.6). Although implementation of these requirements by integration and maintenance service providers can be different, the requirements apply equally to both. Support for these requirements means that the service provider can provide them to the asset owner upon request.

The terms and conditions for providing these processes are beyond the scope of this document. In addition, this document can be used by these service providers to structure and improve their security programs.

In addition, service providers can use IEC 62443-3-3 and IEC 62443-4-2 in conjunction with this document to work with suppliers of underlying control systems/components. This collaboration can assist the service provider in developing policies and procedures around the capability of a system/component, for example backup and restore based on the recommendations from the suppliers of the systems/components used.

NOTE IACS is a generic expression used to describe an industrial automation and control system (based on the definition taken from IEC TS 62443-1-1), that can be extended to other automation vertical industries. For example: Substation Automation Solutions, smart grid, distributed grid, medical device manufacturing, building automation systems, elevators, and escalators.

The security programs implementing these requirements are expected to be independent of different releases of the control system that is embedded in the Automation Solution. Therefore, a new release of the control system product does not necessarily require a change to the service provider's security program. However, changes to the security program will be required when changes to the underlying control system make the existing security program deficient with respect to these IEC 62443-2-4 requirements.

EXAMPLE 1 A service provider can have experience with a specific control system line of products. Developing policies and procedures for that line of products will be based on the recommendations of the product supplier and the capabilities of the product line. Therefore, when the product capabilities for backup and restore are changed, it is possible the corresponding processes of the service provider's security program (corresponding to SP.12.XX) will need to be changed to remain consistent with the updated product capabilities. On the other hand, the service provider's policies and procedures around non-disclosure agreements or personnel background checks (corresponding to SP.01.03 and SP.01.04) are very likely independent of the control system product used in the Automation Solution.

This collaboration can also be used to improve security in these systems/components. First, the service provider can recommend new or updated security features to the system/component supplier. Second, the service provider can gain knowledge about the system/component that allows it to add its own compensating security measures to the Automation Solution during deployment or maintenance.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2024

The security requirements are specified in Annex A, and are defined in terms of the processes that these security programs are required to provide. Subclause 4.1.4 discusses the ability of industry groups to subset these processes into profiles to address risk reduction. See IEC 62443-3-2 for more detail on security risks.

This document also recognizes that security programs evolve and that processes go through a lifecycle of their own, often starting as completely manual and evolving over time to become more formal, more consistent, and more effective. Subclause 4.2 addresses this issue of evolving processes by defining a maturity model to be used with the application of this document.

EXAMPLE 2 A specific capability might be introduced as a set of manual procedures and then later supplemented with automated tools.

As a result, the requirements in Annex A are stated abstractly, allowing for a wide range of implementations. Integration service provider security program processes that meet these requirements are used during the deployment, configuration, handover, and commissioning of the Automation Solution, while maintenance service providers security program processes are used to update and maintain the security of the Automation Solution once it becomes operational.

It is expected that service providers and asset owners will negotiate and agree on which of these required processes are to be provided and how they are to be provided. These aspects of fulfilling the requirements are beyond the scope of this document, although the use of profiles that are accepted by the asset owner and the service provider could make this easier.

EXAMPLE 3 A service provider can be capable of supporting complex passwords and also be capable of supporting specific variations of complex passwords as defined by the password policies of asset owners.

EXAMPLE 4 Many processes have a timeliness aspect related to their performance that is agreed to by both the asset owner and the service provider.

4.1.2 Use of this document by asset owners

This document can be used by asset owners to request specific security processes from the service provider. More specifically, prior to such a request, this document can be used by asset owners to determine whether or not a specific service provider’s security program includes the processes that the asset owner needs.

In general, this document recognizes that asset owner requirements vary, so it has been written to encourage service providers to implement the required processes so that they can be adaptable to a wide variety of asset owners. For example, the asset owner can evaluate whether the service provider’s security-related processes comply with the requirements of this document, or the service provider can use a generic or "reference" architecture applicable to the asset owner system to demonstrate its security program processes to the asset owner. Many technical security capabilities may exist within a reference architecture that can be applied to the Automation Solution during its integration, commissioning, and maintenance cycles. The service provider's security program defines processes that can be performed to adapt and match the Automation Solution to asset owner needs.

The maturity model also allows asset owners to better understand the maturity of a specific service provider’s processes.

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 62443-2-4:2024

4.1.3 Use of this document during negotiations between asset owners and IACS service providers

Prior to the service provider starting work on the Automation Solution, the asset owner normally issues a Request for Quote (RFQ) that includes a set of documents (e.g. a Statement/Scope of Work – SOW) that describes its security policies and defines its security program requirements (see Annex A). See IEC 62443-3-2 for more information on asset owner security requirements applied during system design. Service providers respond to the RFQ and negotiations follow in which the service provider and the asset owner come to agreement on the details of the SOW (or similar document). Typically, the specific responsibilities and processes of the service provider for supporting asset owner security policies and requirements will be included in or referenced by this agreement/contract between the IACS service provider and the asset owner.

NOTE When the service provider is part of the asset owner's organization, it is possible such contract does not exist.

In the event that the asset owner does not specify how to implement its security requirements, the service provider should follow the processes required by this document. However, the asset owner may still specify constraints and parameters for implementation, which should be taken into account when following the service provider's processes during the project. In cases where the asset owner does not specify security requirements, the service provider may propose them to the asset owner based on its own security analysis, and then negotiate which are included in the SOW.

It is also expected that the service provider will have some ability to customize its processes to meet the needs of the asset owner. However, specification of this customization is beyond the scope of this document.

4.1.4 Profiles

This document recognizes that not all of the requirements in Annex A apply to all industry sectors/environments. To allow subsetting and adaptation of these requirements, this document provides for the use of "Profiles".

IEC Technical Reports (TRs) can be created by industry groups/sectors or other organizations to define Profiles for guidance purposes by following ISO/IEC Directives, Part 1 and Part 2. See IEC 62443-1-5[1] Scheme for IEC 62443 cyber security profiles for information on creating profiles.

Each IEC TR can define one or more Profiles, and each Profile identifies a subset of the requirements defined in Annex A and specifies, where necessary, how specific requirements are to be applied in the environment where they are to be used. An IEC TR cannot supersede this document, or add to or modify its security requirements.

It is anticipated that asset owners will select these Profiles to specify the requirements that apply to their Automation Solutions.

4.1.5 Integration service providers

The integration service provider is a type of service provider that performs activities to implement/deploy Automation Solutions for asset owners. This document defines requirements for security processes that the integration service provider can perform as part of or in parallel these activities.

Integration service provider activities generally start with the beginning of the deployment of the Automation Solution and end when the Automation Solution becomes operational.

---

[1] Under preparation. Stage at the time of publication: IEC TS/APUB 62443-1-5:2023.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2024

NOTE 1 The integration service provider can be a role within the asset owner's organization.

IACS integration service provider activities typically include

a) analyzing the physical, electrical, or mechanical environment the Automation Solution is to control (e.g. the physical process to be controlled, such as those used in manufacturing, refining and pharmaceutical processes);
b) developing an Automation Solution architecture in terms of devices and control loops and their interconnectivity with engineering and operator workstations, and possibly the inclusion of a Safety Instrumented System (SIS);
c) defining how the Automation Solution will connect to external (e.g. plant) networks;
d) installing, configuring, patching, backing up, and testing that lead to the handover of the Automation Solution to the asset owner for operation;
e) gaining approval of the asset owner for many of the decisions made and outputs generated during the execution of these activities;

This description of integration service provider activities is abstract and can exclude some of these activities or include other activities that generally precede the handover of the Automation Solution. Also, these activities include participation with the asset owner to ensure the asset owner requirements are met.

From the perspective of the IEC 62443 series, integration service providers are expected to be able to work with the asset owner to identify Automation Solution security risks, and to be able to use the results of such an assessment provided by the asset owner. The service provider is also expected to be able to use processes required by this document in its security program to address these risks.

NOTE 2 See IEC 62443-3-2 for guidance on the use of risk assessments and the definition of security requirements.

4.1.6 Maintenance service providers

The maintenance service provider is a type of service provider that performs activities to maintain and service Automation Solutions for asset owners. They are separate from activities used to operate the Automation Solution. This document defines requirements for security processes that the maintenance service provider can perform as part of or in parallel with these maintenance activities.

Maintenance activities generally fall into two categories: those that apply specifically to maintaining the security of the Automation Solution, and those that apply to maintaining other aspects of the Automation Solution, such as device and equipment maintenance, but that have the responsibility to ensure that security is not degraded as a result of these activities.

NOTE 1 The maintenance service provider is a role that can be within the asset owner's organization.

NOTE 2 There can be one or more maintenance service providers maintaining the Automation Solution at the same time or in sequence.

Maintenance activities generally start once the Automation Solution becomes operational and continue until the asset owner no longer requires them. They are typically short and frequently recurring, and typically include one or more of the following:

a) patching and anti-virus updates;
b) equipment upgrades and maintenance, including small engineering adjustments not directly related to control algorithms;
c) component and system migration;
d) change management;
e) contingency plan management.

AVA Documents Document Sharing Hub

Full document details: BS EN IEC 62443-2-4:2024

All maintenance activities include some level of security awareness independent of whether or not they are directly security related. No activity should reduce the security posture of the Automation Solution after it has been completed.

This description of maintenance activities is abstract and can include other activities generally following the handover of the Automation Solution. Also, these activities include participation with the asset owner to ensure the asset owner's requirements are met.

From the perspective of the IEC 62443 series, maintenance service providers are expected to be able to work with the asset owner to identify Automation Solution security risks, and to be able to use the results of such an assessment provided by the asset owner. The service provider is also expected to be able to use processes required by this document in its security program to address these risks.

NOTE 3 See IEC 62443-3-2 for guidance on the use of risk assessments and the definition of security requirements.

4.2 Maturity model

The requirements specified in Annex A can be implemented in an evolutionary manner by a service provider. Subclause 4.2 defines a maturity model that sets benchmarks for meeting these requirements.

These benchmarks are defined by maturity levels as shown in Table 1. The maturity levels are based on the CMMI® for Services (CMMI-SVC) model, defined in CMMI for Services, Version 1.3. Table 1 shows the relationship to the CMMI-SVC in the "Description/Comparison with CMMI-SVC" column.

Each maturity level is progressively more advanced than the previous level and applies independently for each base requirement (BR) and for each requirement enhancement (RE) in Table A.1. The maturity level is an indicator of how evolved (mature) the process is that implements the BR or RE. Service providers are required to identify the maturity level associated with their implementation of each BR and RE. This makes it possible for asset owners to determine, in measurable terms, the maturity level of a specific service provider's processes.

NOTE 1 Industry groups/sectors can identify specific maturity levels for themselves to better meet their individual needs.

NOTE 2 It is intended that, over time and for a specific requirement, a service provider's processes will evolve to higher levels as it gains proficiency in meeting the requirement.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2024

Table 1 – Maturity levels

Level	CMMI-SVC	IEC 62443-2-4	IEC 62443-2-4 description/comparison to CMMI-SVC
1	Initial	Initial	At this level, the models are fundamentally the same. Service providers typically perform the service in an ad-hoc and often undocumented (or not fully documented) manner. Requirements for the service are typically specified in a statement of work under contract with the asset owner. As a result, consistency across projects is not always be able to be shown. NOTE "Documented" in this context refers to the procedure followed in performing this service (e.g. detailed instructions to service provider personnel), not to the results of performing the service. In most asset owner settings, all changes resulting from the performance of a services task are documented.
2	Managed	Managed	At this level, the models are fundamentally the same, with the exception that this document recognizes that there can be a significant delay between defining a service and executing (practicing) it. Therefore, the execution related aspects of the CMMI-SVC Level 2 are deferred to Level 3. At this level, the service provider has the capability to manage the delivery and performance of the service according to written policies (including objectives). The service provider also has evidence to show that personnel who will perform the service have the expertise, are trained, and/or are capable of following written procedures to perform the service. The service discipline reflected by maturity level 2 helps to ensure that service practices are repeatable, even during times of stress. When these practices are in place, their execution will be performed and managed according to their documented plans.
3	Defined	Defined (Practiced)	At this level, the models are fundamentally the same, with the exception that the execution related aspects of the CMMI-SVC Level 2 are included here. Therefore, a service at Level 3 is a Level 2 service that the service provider has practiced for an asset owner at least once. The performance of a Level 3 service can be shown to be repeatable across the service provider's organization. Level 3 services can be tailored for individual projects based upon the contract and statement of work from the asset owner.
4	Quantitatively Managed Optimizing	Improving	At this level, this document combines CMMI-SVC Levels 4 and 5. Using suitable process metrics, service providers control the effectiveness and performance of the service and demonstrate continuous improvement in these areas, such as more effective procedures or the installation of system capabilities with higher security levels (see IEC 62443-3-3). This results in a security program that improves the service through technological/procedural/management changes.

5 Requirements overview

5.1 Contents

Annex A contains the list of security program requirements for IACS integration and maintenance service providers. They are specified as a list of base requirements (BR) and requirements enhancements (RE) presented in Table A.1. BRs and REs are described in 5.5.2. Each specifies a capability that the service provider can offer to the asset owner during integration and maintenance activities.

Not all requirements apply to all service providers, and asset owners can request service providers to perform only a subset of the required processes specified in Annex A. In addition, industry sectors, service providers, and asset owners can define their own profiles that contain a subset of these requirements (see 4.1.4).

NOTE Industry groups/sectors can subset the requirements to better meet their individual needs.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2024

5.2 Sorting and filtering

The columns in Table A.1 have been designed to be easily sorted and filtered electronically using the spreadsheet version of that table that is distributed with this document. This allows different readers to organize the requirements according to their needs. The column values used for sorting and filtering are defined in 5.5.

5.3 IEC 62264-1 hierarchy model

Many of the requirements in Annex A refer to network or application levels in phrases such as "a wireless handheld device is used in Level 2". When capitalized, "Level" in this context refers to the position in the IEC 62264-1 Hierarchy Model. The Level of a referenced object (e.g. wireless handheld device) is represented by the lowest Level function that it executes. The zones and conduits model described by IEC 62443-3-2 is referenced by requirements in Annex A that address, independent of the IEC 62264-1 Hierarchy Model Level, trust boundaries that subdivide the Automation Solution into partitions referred to as "zones" by IEC 62443-3-2.

NOTE 1 The Hierarchy Model contained in IEC 62264-1:2013, is also known as the Purdue Reference Model and is also specified by ISA 95, Enterprise-Control System Integration.

NOTE 2 In addition to Annex A requirements, industry/group sectors can define their own requirements that are outside the scope of this document to better meet their individual needs.

5.4 Requirements table columns

The columns used in Table A.1 are defined in Table 2. The values for these columns are defined in 5.5.

Table 2 – Columns

Column	Column description
Reb ID	Requirement ID
BR/RE	Base requirement/requirement enhancement indicator
Functional area	Keyword representing the main functional area of a requirement
Topic	Keyword representing the main topic associated with a requirement. The same topic can apply to more than one functional area.
Subtopic	Keyword representing the subtopic addressed by the requirement. The same subtopic can apply to more than one functional area and/or activity.
Doc?	Deliverable documentation is required to be provided to the asset owner (yes/no). NOTE Some requirements can require the service provider to maintain documentation that is not considered a deliverable. However, the asset owner can have agreements with the service provider to see or have this documentation delivered to it.
Requirement description	The text of the requirement.
Rationale	Text that describes the background, justification, and other aspects of the requirement to assist the reader in its understanding

5.5 Column definitions

5.5.1 Req ID column

This column contains the Security Program Requirement Identifier. The same Req ID identifies a base requirement and its requirement enhancements. This identifier is structured into three parts separated by dots ("."):

1) "SP", indicating "Security Program";
2) two-digit identifier for the functional area (see Table 3 for values);
3) two-digit identifier for the requirement, assigned numerically within the Functional Area.

AVA Documents Document Sharing Hub

Full document details: BS EN IEC 62443-2-4:2024

Base requirements and their requirement enhancements all have the same SP Requirement Identifier. See 5.5.2 for the description of base requirements and requirement enhancements.

5.5.2 BR/RE column

This column indicates whether the requirement is a Base Requirement (BR) or a Requirement Enhancement (RE).

- Base requirements

  Base requirements are considered fundamental requirements for all security programs. They are generally abstract in nature to allow service providers latitude in their implementations.

- Requirement enhancements

  Requirement enhancements generally restrict or specialize (i.e. make more specific) base requirements or enhanced requirements. Requirement enhancements on base requirements provide one level of restriction/specialization of the base requirement, while requirement enhancements on other requirement enhancements provide even higher levels of restrictions/specializations on the base requirement. The intent of these restrictions/specializations is to enhance security through the application of more sophisticated security processes or by more rigorous application of these processes.

- Requirement implementation

  A service provider that implements a capability defined by a base requirement can choose from a wide variety of implementations to meet the requirement. A service provider that implements a capability defined by a requirement enhancement, on the other hand, has a restricted range of implementations that can be used.

- Requirement numbering

  Both the base requirement and its enhancements share the same SP Req ID (see 5.5.1). Requirement enhancements are numbered sequentially starting at 1 for each base requirement.

  Requirement enhancements are numbered sequentially starting at "1" for each BR and this sequence number is placed in parentheses following the "RE". Therefore, the column value is RE(#), where # is the sequence number of the enhancement. Requirement enhancements that enhance other requirement enhancements are numbered higher than the enhancements they enhance.

EXAMPLE 1 SP.01.02 BR is a base requirement for assigning personnel to the Automation Solution who have been informed of this document's security requirements, and RE(1) enhances that requirement by defining a requirement for background checks of service provider personnel assigned to the Automation Solution. The BR says that the service provider is able to assign anyone to the Automation Solution who has been trained on the requirements of this document, while RE(1) says that they can only assign trained personnel who have passed background checks.

EXAMPLE 2 SP.01.02 RE(2) defines an enhancement for the RE(1) requirement by specializing the RE(1) requirement to apply to subcontractor personnel assigned to the Automation Solution.

5.5.3 Functional area column

This column provides the top-level technical organization of the requirements. Table 3 provides a list of the functional areas. The functional areas in this column can be used to provide a high-level summary of the areas in which service providers claim conformance. However, because the "Architecture" functional area is so broad, its use as a summary level is limited. Therefore, it is subdivided into three summary levels based on the Topic column (see 5.5.4) values for Architecture as shown in Table 4.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2024

Table 3 – Functional area column values

Value	SP Req ID	Description
Solution staffing	SP.01.XX	Requirements related to the assignment of personnel by the service provider to Automation Solution related activities
Assurance	SP.02.XX	Requirements related to providing confidence that the Automation Solution security policy is enforced
Architecture	SP.03.XX	Requirements related to the design of the Automation Solution
Wireless	SP.04.XX	Requirements related to the use of wireless in the Automation Solution
SIS	SP.05.XX	Requirements related to the integration of SIS into the Automation Solution
Configuration management	SP.06.XX	Requirements related to the configuration control of the Automation Solution
Remote access	SP.07.XX	Requirements related to the remote access to the Automation Solution
Event management	SP.08.XX	Requirements related to the event handling in the Automation Solution
Account management	SP.09.XX	Requirements related to the administration of user accounts in the Automation Solution
Malware protection	SP.10.XX	Requirements related to the use of anti-malware software in the Automation Solution
Patch Management	SP.11.XX	Requirements related to the security aspects of approving and installing software patches
Backup/Restore	SP.12.XX	Requirements related to the security aspects of backup and restore

Table 4 – Architecture Functional Area Summary Levels

Summary Level	Topic column	SP Identifiers
Network Security	Devices – Network	SP.03.08 BR, SP.03.08 RE(1), SP.03.08 RE(2), SP.03.08 RE(3)
	Network design	SP.03.02 BR, SP.03.02 RE(1), SP.03.02 RE(2), SP.03.03 RE(1), SP.03.04 BR
Solution Hardening	Devices – All	SP.03.05 BR, SP.03.05 RE(1)
	Devices – Workstations	SP.03.06 BR, SP.03.07 BR, SP.03.07 RE(1)
	Risk assessment	SP.03.01 BR, SP.03.01 RE(1), SP.03.01 RE(2)
	Solution components	SP.03.03 BR
Data Protection	Data Protection	SP.03.09 BR, SP.03.10 BR, SP.03.10 RE(1), , SP.03.10 RE(2), , SP.03.10 RE(3), , SP.03.10 RE(4),

5.5.4 Topic column

This column contains the keyword that best describes the major topic addressed by the requirement. Topic keywords are independent of functional areas to allow filtering to be used to find all requirements with the same topic, independent of functional area. Table 5 provides a list of the values for this column.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2024

Table 5 – Topic column values

Value	Description
Accounts – …	Requirements related to the various types of user accounts
Security tools and software	Requirements related to application software and tools used in the Automation Solution for security purposes
Background checks	Requirements related to background checks
Backup	Requirements related to backing up and restoring the Automation Solution from a backup
Data protection	Requirements related to protecting data
Devices – …	Requirements related to the various types of devices used in the Automation Solution
Events – …	Requirements related to the various types of events used in the Automation Solution (e.g. security-related, security compromises, alarms and events)
Hardening guidelines	Requirements related to guidelines that describe how to harden the Automation Solution
Manual process	Requirements related to manual procedures used to provide security-related processes (e.g. patch management, backup/restore)
Network design	Requirements related to the design of the network architecture of the Automation Solution
Passwords	Requirements related to account passwords
Patch list	Requirements related to a list of identifiers and properties of security patches that are applicable to the Automation Solution
Personnel assignments	Requirements related to the assignment of personnel to the Automation Solution
Portable media	Requirements related to the use of portable media in the Automation Solution
Restore	Requirements related to restoring the Automation Solution from a backup
Risk assessment	Requirements related to performing risk assessments for the Automation Solution and its components
Security tools and software	Requirements related to the tools/software used in the implementation and management of security within the Automation Solution
Solution components	Requirements related to components used in the Automation Solution
Training	Requirements related to training for personnel assigned to the Automation Solution
User interface	Requirements related to user interfaces of the Automation Solution
Vulnerabilities	Requirements related to security vulnerabilities in the Automation Solution

5.5.5 Subtopic column

This column contains the keyword that best describes the technical topic associated with the requirement. Technical topic keywords are independent of functional areas and activities to allow filtering to be used to find all requirements with the same technical topic, independent of functional area or activity. Table 6 provides a list of the values for this column.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2024

Table 6 – Subtopic column values

Value	Description
Access control	Requirements related to authentication and/or authorization
Administration	Requirements related to administration and management activities, such as device administration and account management
Approval	Requirements related to obtaining approvals from the asset owner
Change	Requirements related to the changing of passwords
Communications	Requirements related to internal and external communications of the Automation Solution
Composition	Requirements related to the composition of passwords
Configuration mode	Requirements related to the state of a device that allows it to be configured
Connectivity	Requirements related to the network connectivity of devices and/or network segments
Cryptography	Requirements related to the use of cryptographic mechanisms (e.g. encryption, digital signatures)
Data/event retention	Requirements related to archiving of data and events
Delivery	Requirements related to the delivery of security patches
Detection	Requirements related to the detection of events
Disaster recovery	Requirements related to disaster recovery
Expiration	Requirements related to the expiration of accounts and passwords
Installation	Requirements related to the installation of security related tools and software
Inventory register	Requirements related to document that summarizes the devices and their software components that are used in the Automation Solution
Least functionality	Requirements related to supporting the concept of least functionality (e.g. the disabling of an unnecessary service or removal of a temporary account no longer being used). See IEC 62443-3-3 for more detail on least functionality
Logging	Requirements related to audit and event logs
Malware definition files	Requirements related to the approval and use of malware definition files
Malware protection mechanism	Requirements related to the use of malware protection mechanisms (e.g. anti-virus software, whitelisting software)
Network time	Requirements related to the distribution and synchronization of time over the network
Patch qualification	Requirements related to the evaluation and approval of patches for use in the Automation Solution
Perform	Requirements related to performing a capability for the Automation Solution
Reporting	Requirements related to reporting of events (e.g. notifications)
Responding	Requirements related to handling and responding to events
Reuse	Requirements related to the reuse of passwords
Robustness	Requirements related to the ability of the Automation Solution and its components to withstand abnormal data, abnormal sequences, or abnormally high volumes of network traffic, such as alarm storms and network scans
Sanitizing	Requirements related to cleaning devices and portable media of sensitive data and/or malware
Security contact	Requirements that define and require the "security contact" role
Security lead	Requirements that define and require the "security lead" role
Security requirements – …	Requirements related to security requirements contained in this specification or defined by the asset owner
Sensitive data	Requirements related to data requiring safeguarding
Service provider	Requirements related to service provider personnel or their capabilities
Session lock	Requirements related to locking the keyboard and screen of workstations

AVA Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2024

Value	Description
Shared	Requirements related to the sharing of passwords
Subcontractor	Requirements related to personnel or capabilities of the service provider's subcontractors, consultants, or representatives
Technical description	Requirements related to descriptions of some technical aspect of the Automation Solution
Usage	Requirements related to the use or application of a required capability
Verification	Requirements related to verification of a capability (e.g. via a demonstration or visual inspection)
Wireless network identifiers	Requirements related to identifiers for wireless networks

5.5.6 Documentation column

This column contains a Yes to indicate that the requirement describes a capability that requires deliverable documentation to the asset owner. Requirements with a No value may require that the service provider create and/or maintain documentation in support of the required capability, but this documentation is not considered to be deliverable to the asset owner. However, in separate agreements, the asset owner can request any documentation to be regarded as deliverable.

5.5.7 Requirement description column

This column contains the textual description of the requirement. It may also contain notes that are examples provided to help in understanding the requirement.

Each row in Table A.1 specifies a requirement for a process that the service provider can perform for the asset owner for the integration, commissioning or maintenance of the Automation Solution. The text of each requirement description, therefore, begins with "The service provider shall have a process that can be performed for the asset owner to…". Whether an asset owner requires the service provider to perform the process is beyond the scope of this document. To be compliant with a requirement, the service provider's process can be conformant to any of the four maturity levels defined in 4.2.

The term "ensure" is used in many requirements to mean "make certain that the result specified by the requirement is achieved". In many requirements, "ensure" is used to require that the service provider has a process to apply and use a technical capability to the Automation Solution. The specified result can be achieved through such actions as configuration, demonstration, verification, and testing. How the service provider actually ensures that the required result is achieved is not specified in order to maintain implementation independence and to make allowances for the differences between integration and maintenance provider processes. However, the Rationale column (see 5.5.8) is used to provide guidance where needed.

The phrase "commonly accepted by both the security and industrial automation communities" is used in these requirement descriptions in place of specific security technologies, such as specific encryption algorithms. This phrase is used to allow evolution of more secure technologies as a replacement for technologies whose weaknesses have been exposed.

To be compliant with these requirements, service providers will have to use technologies (e.g. encryption) that are commonly accepted and used by the security and industrial automation communities at the time compliance is claimed. Technologies that are no longer considered secure, such as the Data Encryption Standard (DES) and the Wired Equivalent Privacy (WEP) security algorithms, would be non-conformant.

AVA Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2024

5.5.8 Rationale column

This column contains the rationale that describes the reasoning behind each requirement (i.e. purpose/benefit of the required capability) and provides supplemental guidance for a better understanding of each requirement. In many of the descriptions, the terminology "has an identifiable process" is used. "Identifiable" means that the service provider has a process that it can use and that it can make known to (identify) and perform for the asset owner. The application of the maturity model described in 4.2 can mean that this process has not yet been formally documented (maturity level 1).

Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2024

Annex A
(normative)

Security requirements

Table A.1 – Security program requirements

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.01.01	BR	Solution staffing	Training	Security requirements – IEC 62443-2-4	No	The service provider shall have a process that can be performed for the asset owner that it assigns only service provider personnel to Automation Solution related activities who have been informed of and comply with the requirements defined in this document that are required by the asset owner.	The capabilities specified by this BR and its REs are used to protect the Automation Solution from threats initiated by service provider, subcontractor, and consultant personnel who are not aware of their standard security responsibilities (i.e. security best practices). All too often, security compromises are the result of personnel taking an action without realizing they are violating a security best practice (e.g. plugging in an unauthorized USB memory stick) or failing to take an appropriate action (e.g. failure to update a perimeter firewall rule after removing an external workstation). Meeting this requirement means that the service provider is able to provide service provider personnel to work on the Automation Solution who are aware of the security requirements defined in this document that the asset owner requires to be implemented in the IACS. Approaches for informing personnel generally include training and/or review of procedures. NOTE 1 Asset owners can ask for acknowledgment of training in writing. NOTE 2 Maturity levels 3 and 4 (see 4.2) are applicable to the enforcement of (complying with) the responsibilities, policies, and procedures.
SP.01.01	RE(1)	Solution staffing	Training	Security requirements – IEC 62443-2-4	No	The service provider shall have a process that can be performed for the asset owner to assign only subcontractor or consultant personnel to Automation Solution related activities who have been informed of and comply with requirements defined in this document that are required by the asset owner.	Meeting this requirement means that the service provider is able to provide subcontractor personnel, consultants, and representatives to work on the Automation Solution who are aware of the security requirements defined in this document that the asset owner requires to be implemented in the IACS. See ISO/IEC 27036-3 for additional supply chain organizational requirements.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2024