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 62443-2-4:2019+A1:2019

National foreword

This British Standard is the UK implementation of EN IEC 62443-2-4:2019+A1:2019. It is identical to IEC 62443-2-4:2015+A1:2017.

The start and finish of text introduced or altered by amendment is indicated in the text by tags. Tags indicating changes to IEC text carry the number of the IEC amendment. For example, text altered by IEC amendment A1 is indicated by A1 A1.

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 secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2019
Published by BSI Standards Limited 2019

ISBN 978 0 580 95941 7

ICS 35.110; 25.040.40

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 30 June 2019.

Amendments/corrigenda issued since publication

Date	Text affected

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 62443-2-4:2019+A1:2019

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN IEC 62443-2-4:2019/A1

April 2019

ICS 35.110; 25.040.40

English Version

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

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

IT-Sicherheit für industrielle Automatisierungssysteme - Teil 2-4: Anforderungen an das IT-Sicherheitsprogramm von Dienstleistern für industrielle Automatisierungssysteme

This European Standard was approved by CENELEC on 2019-04-03. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

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

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

© 2019 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

Ref. No. EN IEC 62443-2-4:2019/A1:2019 E

AVA Documents Document Sharing Hub

Full document details: BS EN IEC 62443-2-4:2019+A1:2019

European foreword

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

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2020-04-03
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2022-04-03

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

Endorsement notice

The text of the International Standard IEC 62443-2-4:2015 was approved by CENELEC as a European Standard without any modification.

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

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

Foreword to amendment A1

This document (EN IEC 62443-2-4:2019/A1:2019) consists of the text of IEC 62443-2-4:2015/A1:2017 prepared by IEC/TC 65 "Industrial-process measurement, control and automation".

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2020-04-03
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2022-04-03

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

Endorsement notice

The text of the International Standard IEC 62443-2-4:2015/A1:2017 was approved by CENELEC as a European Standard without any modification.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2019+A1:2019

CONTENTS

FOREWORD 3
INTRODUCTION 5
1 Scope 6
2 Normative references 7
3 Terms, definitions, abbreviated terms and acronyms 7
3.1 Terms and definitions 7
3.2 Abbreviations 10
4 Concepts 11
4.1 Use of IEC 62443-2-4 11
4.1.1 Use of IEC 62443-2-4 by IACS service providers 11
4.1.2 Use of IEC 62443-2-4 by IACS asset owners 12
4.1.3 Use of IEC 62443-2-4 during negotiations between IACS asset owners and IACS service providers 12
4.1.4 Profiles 13
4.1.5 IACS integration service providers 13
4.1.6 IACS maintenance service providers 14
4.2 Maturity model 14
5 Requirements overview 16
5.1 Contents 16
5.2 Sorting and filtering 16
5.3 IEC 62264-1 hierarchy model 16
5.4 Requirements table columns 16
5.5 Column definitions 17
5.5.1 Req ID column 17
5.5.2 BR/RE column 17
5.5.3 Functional area column 18
5.5.4 Topic column 19
5.5.5 Subtopic column 20
5.5.6 Documentation column 22
5.5.7 Requirement description column 22
5.5.8 Rationale column 22
Annex A (normative) Security requirements 23
Bibliography 88

Figure 1 – Parts of the IEC 62443 Series 5
Figure 2 – Scope of service provider capabilities 6

Table 1 – Maturity levels 15
Table 2 – Columns 17
Table 3 – Functional area column values 19
Table 4 – Topic column values 20
Table 5 – Subtopic column values 21
Table A.1 – Security program requirements 23

Documents
Document Sharing Hub

Full document details: BS EN IEC 62443-2-4:2019+A1:2019

INTERNATIONAL ELECTROTECHNICAL COMMISSION

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

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

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

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

This publication contains an attached file in the form of an Excel 97-2003 spreadsheet version of Table A.1. This file is intended to be used as a complement and does not form an integral part of the publication.

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

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

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

Documents
Document Sharing Hub

Full document details: BS EN IEC 62443-2-4:2019+A1:2019

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

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

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

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

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

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

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

Documents
Document Sharing Hub

Full document details: BS EN IEC 62443-2-4:2019+A1:2019

INTRODUCTION

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

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

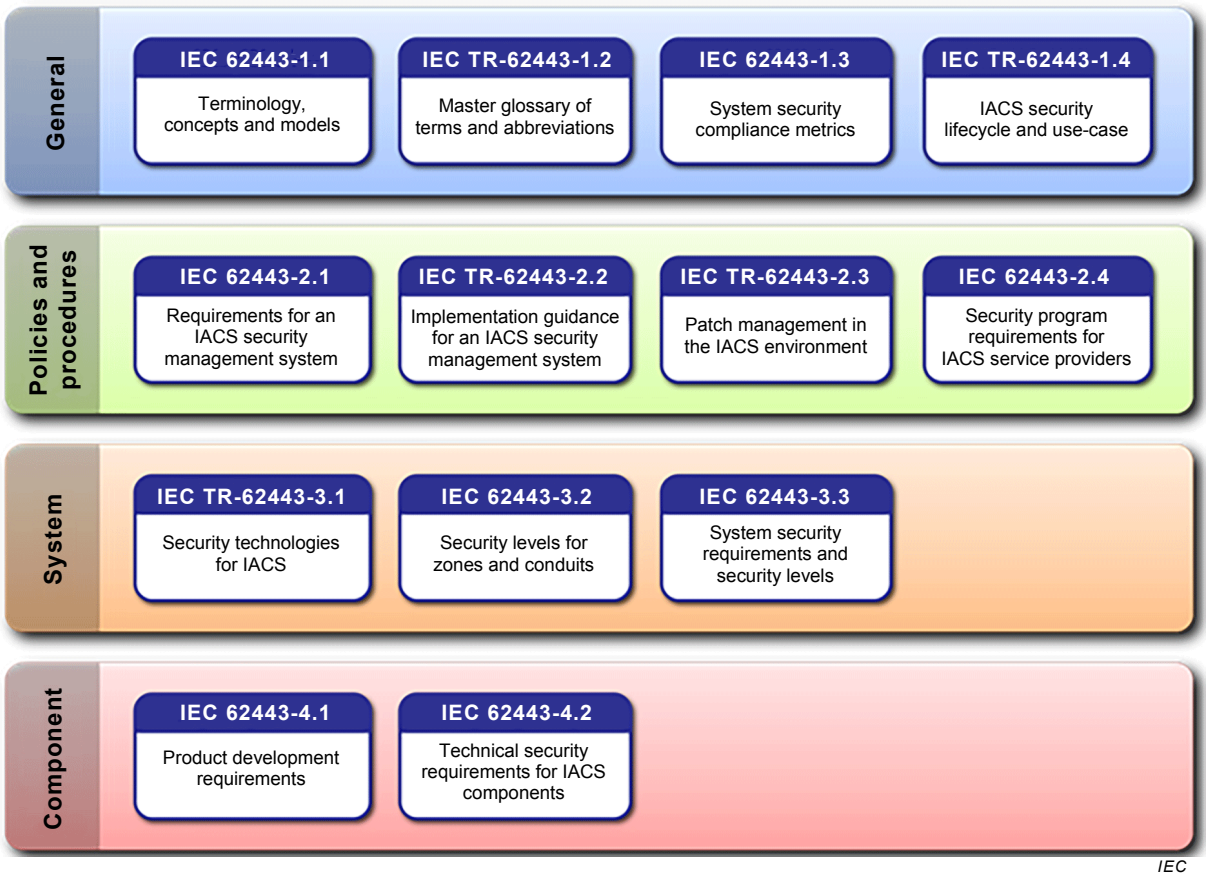

Figure 1 – Parts of the IEC 62443 Series

Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2019+A1:2019

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

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

1 Scope

〈A1〉 This part of IEC 62443 specifies a comprehensive set of requirements for security capabilities for IACS service providers that they can offer to the asset owner during integration and maintenance activities of an Automation Solution. 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. 〈A1〉

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

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

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

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

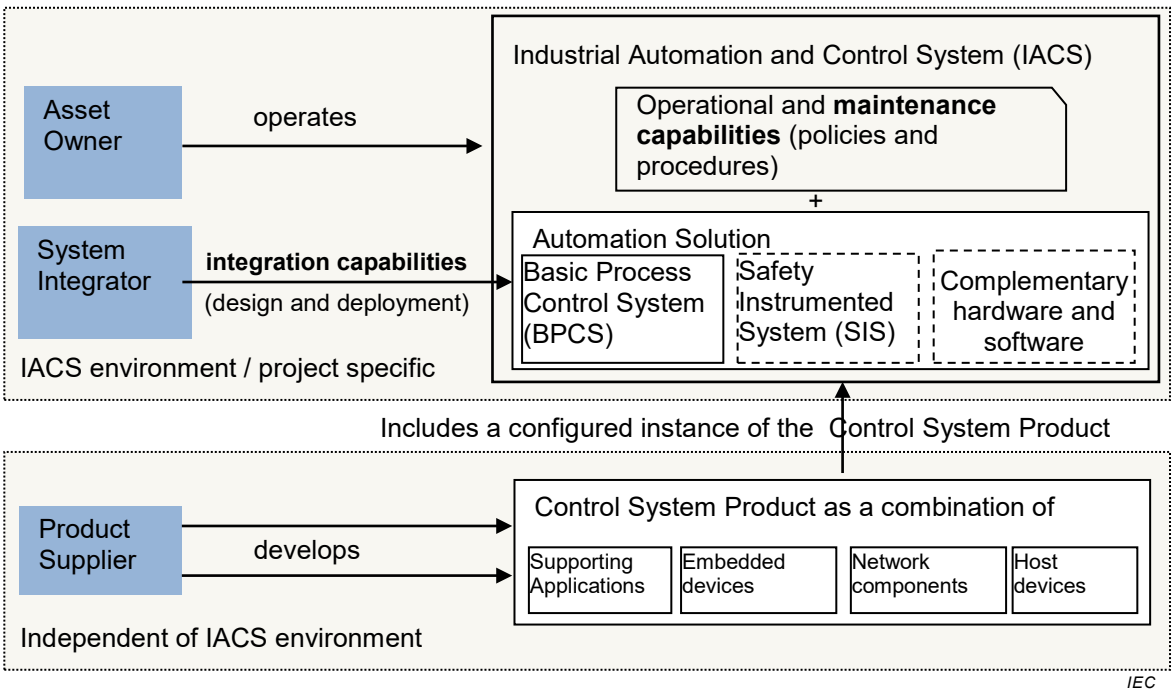

Figure 2 – Scope of service provider capabilities

Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2019+A1:2019

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

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

〈A1〉 *Text deleted* 〈A1〉

NOTE 4 Automation Solutions typically have a single control system (product), but they are not restricted to do so. In general, the Automation Solution is the set of hardware and software, independent of product packaging, that is used to control a physical process (e.g. continuous or manufacturing) as defined by the asset owner.

2 Normative references

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

“None”

3 Terms, definitions, abbreviated terms and acronyms

3.1 Terms and definitions

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

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

Note 1 to entry: Used in place of the generic word end user to provide differentiation.

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

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

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

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

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

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

Note 1 to entry: Automation Solution is used as a proper noun in this part of IEC 62443.

Note 2 to entry: The difference between the control system and the Automation Solution is that the control system is incorporated into the Automation Solution design (e.g. a specific number of workstations, controllers, and devices in a specific configuration), which is then implemented. The resulting configuration is referred to as the Automation Solution.

Note 3 to entry: The Automation Solution may be comprised of components from multiple suppliers, including the product supplier of the control system.

AVA Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2019+A1:2019

3.1.4
basic process control system
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 integrated 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 may apply to a variety of industrial processes, including continuous processes and manufacturing processes.

3.1.5
consultant
subcontractor that provides expert advice or guidance to the integration or maintenance service provider

3.1.6
control system
hardware and software components used in the design and implementation of an IACS

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

3.1.7
handover
act of turning an Automation Solution over to the asset owner

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

3.1.8
industrial automation and control system
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 may include components that are not installed at the asset owner’s site.

Note 2 to entry: The definition of IACS was taken from in IEC-62443-3-3 and is illustrated in Figure 2. Examples of IACSs include Distributed Control Systems (DCS) and Supervisory Control and Data Acquisition (SCADA) systems. IEC 62443-2-4 also defines the proper noun “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.

3.1.9
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).

3.1.10
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, e.g. managing user accounts, security monitoring, and security assessments.

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 62443-2-4:2019+A1:2019

3.1.11
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 / BluRay Media, USB memory devices, smart phones, flash memory, solid state disks, hard drives, handhelds, and portable computers.

3.1.12
product supplier
manufacturer of hardware and/or software product

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

3.1.13
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.

3.1.14
safety instrumented system
system used to implement functional safety

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

〖A1〗Note 2 to entry: Not all industry sectors use this term. 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.〖/A1〗

3.1.15
security compromise
violation of the security of a system such that an unauthorized (1) disclosure or modification of information or (2) denial of service may 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.

3.1.16
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 term “of some significance’ is relative to the environment in which the security compromise is detected. For example, the same compromise may 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.

3.1.17
security patch
software patch 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 may 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 62443-2-4:2019+A1:2019

3.1.18
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.

3.1.19
service provider
individual or 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.

3.1.20
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

3.1.21
system
interacting, interrelated, or interdependent elements forming a complex whole

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

Note 2 to entry: In practice, the interpretation of its meaning 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.

3.1.22
verify
check that the specified requirement was met

3.1.23
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.

3.2 Abbreviations

AES_GCM	Advanced Encryption Standard Galois/Counter Mode
BPCS	Basic Process Control System
BR	Base Requirement
CEF	Common Event Format
DCOM	Distributed Common Object Model
DCS	Distributed Control System
EWS	Engineering Workstation
IACS	Industrial Automation and Control System
RE	Requirement Enhancement
RDP	Remote Desktop Protocol
RFC	Request For Comment
RFQ	Request For Quote

Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2019+A1:2019

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
TR	Technical Report
VPN	Virtual Private Network

4 Concepts

4.1 Use of IEC 62443-2-4

4.1.1 Use of IEC 62443-2-4 by IACS service providers

This part of the IEC 62443 series defines requirements for security capabilities to be supported by security programs of integration and maintenance service providers (see 4.1.3 and 4.1.6). Support for these capabilities means that the service provider can provide them to the asset owner upon request. The terms and conditions for providing these capabilities are beyond the scope of this standard. In addition, IEC 62443-2-4 can be used by these IACS service providers to structure and improve their security programs.

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

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. That is 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 may 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, the corresponding capabilities of the service provider's security program (corresponding to SP.12.XX) may have 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) and 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.

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

AVA Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2019+A1:2019

IEC 62443-2-4 also recognizes that security programs evolve and that capabilities 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. Clause 4.2 addresses this issue of evolving capabilities by defining a maturity model to be used with the application of this standard.

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. It is expected that service providers and asset owners will negotiate and agree on which of these required capabilities are to be provided and how they are to be provided. These aspects of fulfilling the requirements are beyond the scope of IEC 62443-2-4, although the use of profiles should make this easier.

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

EXAMPLE 4 Many capabilities have a timeliness aspect related to their performance. What is considered timely should be agreed to by both the asset owner and the service provider.

4.1.2 Use of IEC 62443-2-4 by IACS asset owners

IEC 62443-2-4 can be used by asset owners to request specific security capabilities from the service provider. More specifically, prior to such a request, IEC 62443-2-4 can be used by asset owners to determine whether or not a specific service provider's security program includes the capabilities that the asset owner needs.

In general, IEC 62443-2-4 recognizes that asset owner requirements vary, so it has been written to encourage service providers to implement the required capabilities so that they can be adaptable to a wide variety of asset owners. The maturity model also allows asset owners to better understand the maturity of a specific service provider's capabilities.

4.1.3 Use of IEC 62443-2-4 during negotiations between IACS asset owners and IACS service providers

Prior to the IACS service provider starting work on the Automation Solution, the asset owner will normally issue a Request for Quote (RFQ)) that includes a document (e.g. a Statement of Work (SOW)) that defines its security policies and requirements, including which of the requirements specified in Annex A apply. See IEC 62443-3-2 for more information on defining security requirements. 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 capabilities 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 1 When the service provider is part of the asset owner's organization, there may not be such a contract.

Additionally, the asset owner does not normally specify how its security requirements (e.g. backup and restore) will be implemented – that is what the service provider has already specified in its policies and procedures. However, the asset owner may define constraints and parameters (e.g. password timeout values) for how the service provider's policies and procedures will be applied in its specific 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 IACS service provider will have some ability to customize its capabilities to meet the needs of the asset owner. However, specification of this customization is beyond the scope of IEC 62443-2-4.

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 62443-2-4:2019+A1:2019

4.1.4 Profiles

〈A1〉 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”.

Profiles are written as IEC Technical Reports (TRs) by industry groups/sectors or other organizations, including asset owners and service providers, to select/adapt Annex A requirements that are most appropriate to their specific needs.

Each TR may 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.

It is anticipated that asset owners will select these profiles to specify the requirements that apply to their Automation Solutions. 〈A1〉

4.1.5 IACS integration service providers

An IACS integration service provider is an organization, typically separate from and under contract to the asset owner that provides capabilities to implement/deploy Automation Solutions according to asset owner requirements. Integration service provider activates generally occur in the time frame starting with the design phase and ending in handover of the Automation Solution to the asset owner.

NOTE 1 The integration service provider can be an organization 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 activates is abstract and may 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 IEC 62443, integration service providers are also expected to participate in the assessment of security risks for the Automation Solution or to use the results of such an assessment provided by the asset owner. The service provider is also expected to use capabilities required by 62443-2-4 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.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2019+A1:2019

4.1.6 IACS maintenance service providers

An IACS maintenance service provider is any organization, typically separate from and under contract to the asset owner, that performs activities to maintain and service Automation Solutions according to asset owner requirements.

Maintenance activities are separate from activities used to operate the Automation Solution and 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 can be an organization 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 after handover of the Automation Solution to the asset owner has occurred and may continue until the asset owner no longer requires them. They are typically short and frequently recurring, and typically include one of 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.

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 after it has been completed.

This description of maintenance activates is abstract and may 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 requirements are met.

From the perspective of the IEC 62443 series, maintenance service providers, like integration service providers, are expected to participate in the assessment of security risks for the Automation Solution (such as for proposed changes) or to use the results of such an assessment provided by the asset owner. The service provider is also expected to use capabilities required by 62443-2-4 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 are open to wide interpretation with respect to how they may be provided by a service provider. This clause 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-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 level is progressively more advanced than the previous level, and applies independently for each requirement in Table A.1. Service providers are required to identify the maturity level associated with their implementation of each requirement. This makes it possible for asset owners to determine in measurable terms, the maturity level of a specific service provider's capabilities.

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 62443-2-4:2019+A1:2019

This model applies to both Base Requirements (BRs) and Requirement Enhancements (REs) defined in Table A.1. REs in this table are extensions of BRs and do not reflect maturity. Instead, REs are defined to provide specializations, restrictions, or generalizations of BRs. They are used in the same way that they are in IEC 62443-3-3.

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

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

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 the 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 may not 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 the fundamentally the same, with the exception that IEC 62443-2-4 recognizes that there may 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. A1 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. A1 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 the 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 may be tailored for individual projects based upon the contract and statement of work from the asset owner.
4	Quantitatively Managed	Improving	At this level, Part 2-4 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. See IEC 62443-1-3 for a discussion of metrics.
5	Optimizing		

Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2019+A1:2019

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.

〈A1〉 Not all requirements apply to all service providers, and asset owners may request service providers to perform only a subset of the required capabilities specified in Annex A. In addition, industry sectors, service providers, and asset owners may define their own profiles that contain a subset of these requirements (see 4.1.4). 〈A1〉

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

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 international standard. 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

〈A1〉 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. 〈A1〉

NOTE The IEC 62264-1 Hierarchy Model is also known as the Purdue Reference Model and is also specified by ISA 95.

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.

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 62443-2-4:2019+A1:2019

Table 2 – Columns

Column	Column description
Req 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 may apply to more than one functional area.
Subtopic	Keyword representing the subtopic addressed by the requirement. The same technical topic may 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 may require the service provider to maintain documentation that is not considered a deliverable. However, the asset owner may 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 (“.”):

- the first part is “SP”, indicating “Security Program”;
- the second part is the two-digit identifier for the functional area (see Table 3 for values);
- the third part is the two-digit identifier for the requirement, assigned numerically within the Functional Area. 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 are generally place restrictions on, or otherwise specialize, the capabilities of 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 more sophisticated security capabilities or by more rigorous application of these capabilities.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2019+A1:2019

Requirement implementation

As a result, a service provider that implements a capability defined by a base requirement may choose 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. In this manner.

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 the IEC 62443-2-4 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 IEC 62443-2-4 requirements, while RE(1) says that they can only assigned 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

〖A1〗 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 below:

Summary Level	Topic column
Network Security	Devices – Network
	Network design
Solution Hardening	Devices – All
	Devices – Workstations
	Risk assessment,
	Solution components
Data Protection	Data Protection 〖A1〗

Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2019+A1:2019

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

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 4 provides a list of the values for this column.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2019+A1:2019

Table 4 – 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 capabilities (e.g. patch management, backup/restore)
Network design	Requirements related to the design of the Automation Solution's network architecture
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 5 provides a list of the values for this column.

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 62443-2-4:2019+A1:2019

Table 5 – 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 its capabilities
Session lock	Requirements related to locking the keyboard and screen of workstations
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

Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2019+A1:2019

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 may request any documentation to be regarded as deliverable.

5.5.7 Requirement description A1 column A1

A1 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 requirement defines a capability required of the service provider. Whether an asset owner requires the service provider to perform the capability is beyond the scope of this document.

The term “ensure” is used in many requirements to mean “provide a high level of confidence”. It is used when the service provider needs to have some means, such as a demonstration, verification, or process, of providing this level of confidence.

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 to 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 Digital Encryption Standard (DES) and the Wireless Equivalent Privacy (WEP) security algorithms, would be non-conformant. A1

5.5.8 Rationale A1 column A1

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 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 means that this process may not yet be formally documented (maturity level 1).

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 62443-2-4:2019+A1:2019

Annex A
(normative)

Security requirements

A1 Table A.1 – Security program A1

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 the capability to ensure that it assigns only service provider personnel to Automation Solution related activities who have been informed of and comply with the responsibilities, policies, and procedures required by this specification.	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). Having this capability means that the service provider is able to provide service provider personnel to work on the Automation Solution who are security-aware. Approaches for informing personnel generally include training and/or review of procedures. NOTE 1 Asset owners may 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 the capability to ensure that it assigns only subcontractor or consultant personnel to Automation Solution related activities who have been informed of and comply with the responsibilities, policies, and procedures required by this specification.	Having this capability means that the service provider is able to provide subcontractor personnel, consultants, and representatives to work on the Automation Solution who are security-aware. See ISO/IEC 27036-3 for additional supply chain organizational requirements.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2019+A1:2019

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.01.02	BR	Solution staffing	Training	Security requirements – asset owner	No	The service provider shall have the capability to ensure that it assigns only service provider, subcontractor or consultant personnel to Automation Solution related activities who have been informed of and comply with the security-related responsibilities, policies, and procedures required by the asset owner.	The capability specified by this BR minimizes threats to the Automation Solution that could be initiated by service provider, subcontractor, and consultant personnel who are not aware of their Automation Solution specific security responsibilities (as defined by the asset owner). All too often, security compromises are the result of personnel not being aware of asset owner defined security requirements (e.g. misusing or improperly sharing a maintenance account). Having this capability means that the service provider has an identifiable process for ensuring that personnel provided to work on the Automation Solution are knowledgeable of and comply with the security requirements of the asset owner. This includes both service provider personnel as well as its subcontractors, consultants, and representatives. Approaches for informing personnel generally include training and/or review of procedures. See ISO/IEC 27036-3 for additional supply chain organizational requirements. NOTE 1 Asset owners may require 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.01.02	RE(1)	Solution staffing	Training	Security requirements – asset owner	No	The service provider shall have the capability to ensure that it assigns only service provider, subcontractor or consultant personnel to Automation Solution related activities who have been informed of and comply with the asset owner's Management of Change (MoC) and Permit To Work (PtW) processes for changes involving devices, workstations, and servers and connections between them.	The capability specified by this RE minimizes threats to the Automation Solution related to service provider personnel having unauthorized access to the Automation Solution and making unauthorized changes to the Automation Solution. Having this capability means that the service provider has an identifiable process for ensuring that personnel provided to work on the Automation Solution are knowledge of and comply with the asset owner's Management of Change (MoC) and Permit To Work (PtW) processes to ensure that changes to devices/workstations/servers are properly managed. NOTE Maturity levels 3 and 4 (see 4.2) are applicable to the enforcement of (complying with) the responsibilities, policies, and procedures.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2019+A1:2019

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.01.03	BR	Solution staffing	Training	Sensitive data	No	The service provider shall have the capability to ensure that it assigns only service provider personnel to Automation Solution related activities who have been informed of and comply with the policies, procedures, and contractual obligations required to protect the confidentiality of the asset owner's data.	The capabilities specified by this BR and its REs are used to protect the Automation Solution from the mishandling of asset owner data and thus allowing its disclosure (e.g. printing a recipe and leaving it unattended or visible to bystanders). Having this capability means that the service provider is able to provide personnel to work on the Automation Solution who are aware of their responsibility to protect the asset owner's proprietary data from disclosure. It is typical for non-disclosure agreements (NDA) to be used to define the terms related to protecting confidential data, including what data to protect and which special handling requirements exist. Having this capability additionally requires the service provider to have an identifiable process for informing its personnel of the existence and conditions of such a non-disclosure agreement. In addition, asset owners may require some form of evidence (e.g. in writing) that personnel have been informed of these responsibilities. See ISO/IEC 27036-3 for additional supply chain organizational requirements between the asset owner and the service provider. NOTE Maturity levels 3 and 4 (see 4.2) are applicable to the enforcement of (complying with) the responsibilities, policies, and procedures.

Documents
Document Sharing Hub
Full document details: BS EN IEC 62443-2-4:2019+A1:2019

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.01.03	RE(1)	Solution staffing	Training	Sensitive data	No	The service provider shall have the capability to ensure that it assigns only subcontractors, consultants, and representatives to Automation Solution related activities who have been informed of and comply with the policies and procedures required to protect the confidentiality of the asset owner's data.	Having this capability means that the service provider is able to ensure that subcontractor, consultant, and representatives who are assigned to work on the Automation Solution are aware of their responsibility to protect the asset owner's proprietary data from disclosure. It is typical for non-disclosure agreements (NDA) to be used to define the terms related to protecting confidential data, including what data to protect and which special handling requirements exist. Having this capability additionally requires the service provider to have an identifiable process for informing these personnel of the existence and conditions of such a non-disclosure agreement. In addition, asset owners may require some form of evidence (e.g. in writing) that personnel have been informed of these responsibilities. See ISO/IEC 27036-3 for additional supply chain organizational requirements between the asset owner and the service provider. NOTE Maturity levels 3 and 4 (see 4.2) are applicable to the enforcement of (complying with) the responsibilities, policies, and procedures.

© IEC 2017

Documents
Document Sharing Hub

Full document details: BS EN IEC 62443-2-4:2019+A1:2019