IEC 62443-2-4

Edition 1.1 2017-08

CONSOLIDATED VERSION

colour inside

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

IEC 62443-2-4:2015-06+AMD1:2017-08 CSV(en)

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

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

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

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

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

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 It also gives information on projects, replaced and withdrawn publications.

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

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

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

IEC 62443-2-4

Edition 1.1 2017-08

CONSOLIDATED VERSION

colour inside

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 25.040.40; 35.110

ISBN 978-2-8322-4679-5

Warning! Make sure that you obtained this publication from an authorized distributor.

IEC 62443-2-4

Edition 1.1 2017-08

REDLINE VERSION

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

IEC 62443-2-4:2015-06+AMD1:2017-08 CSV(en)

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

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

FOREWORD

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

DISCLAIMER
This Consolidated version is not an official IEC Standard and has been prepared for user convenience. Only the current versions of the standard and its amendment(s) are to be considered the official documents.

This Consolidated version of IEC 62443-2-4 bears the edition number 1.1. It consists of the first edition (2015-06) [documents 65/545/CDV and 65/561A/RVC] and its corrigendum 1 (2015-08), and its amendment 1 (2017-08) [documents 65/637A/CDV and 65/661/RVC]. The technical content is identical to the base edition and its amendment.

In this Redline version, a vertical line in the margin shows where the technical content is modified by amendment 1. Additions are in green text, deletions are in strikethrough red text. A separate Final version with all changes accepted is available in this publication.

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.

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 the base publication and its amendment 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

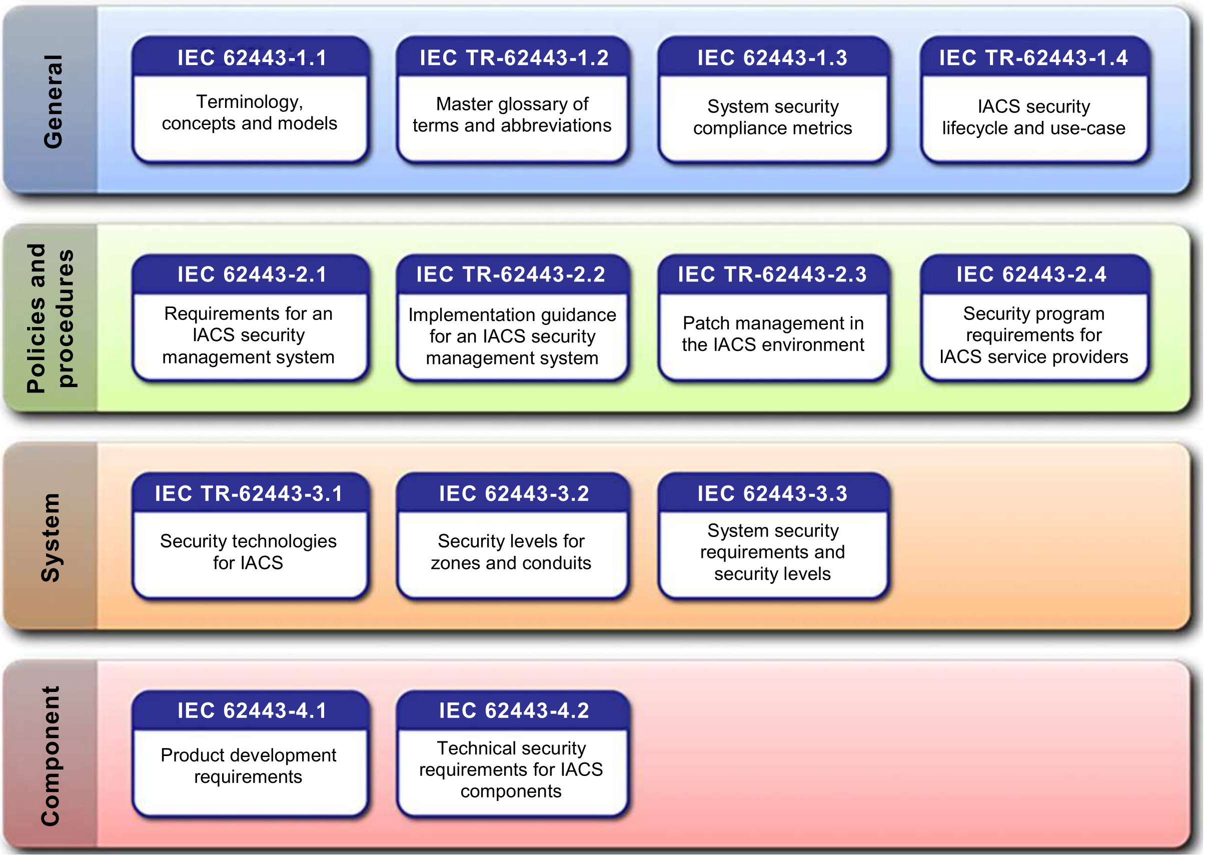
- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

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

INTRODUCTION

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

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


General
IEC 62443-1.1
Terminology, concepts and models
IEC TR-62443-1.2
Master glossary of terms and abbreviations
IEC 62443-1.3
System security compliance metrics
IEC TR-62443-1.4
IACS security lifecycle and use-case
Policies and procedures
IEC 62443-2.1
Requirements for an IACS security management system
IEC TR-62443-2.2
Implementation guidance for an IACS security management system
IEC TR-62443-2.3
Patch management in the IACS environment
IEC 62443-2.4
Security program requirements for IACS service providers
System
IEC TR-62443-3.1
Security technologies for IACS
IEC 62443-3.2
Security levels for zones and conduits
IEC 62443-3.3
System security requirements and security levels
Component
IEC 62443-4.1
Product development requirements
IEC 62443-4.2
Technical security requirements for IACS components

IEC

Figure 1 – Parts of the IEC 62443 Series

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

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

1 Scope

This part of IEC 62443~~-2-4~~ specifies 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.

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).

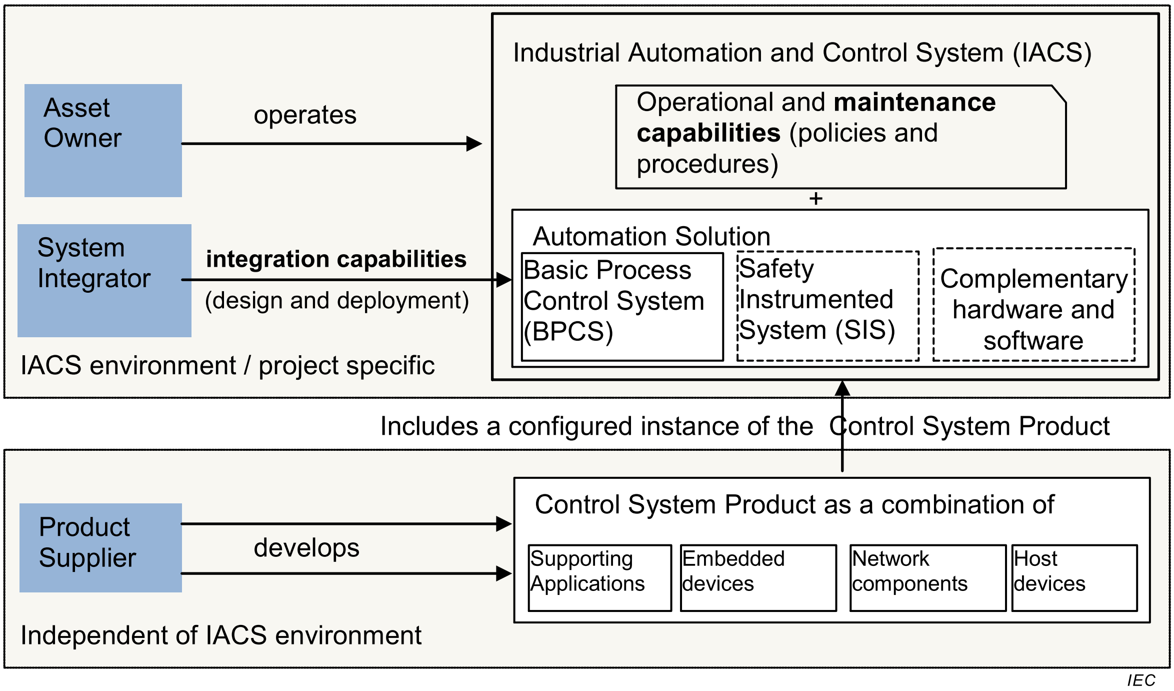

Industrial Automation and Control System (IACS)
Asset Owner
operates
Operational and maintenance capabilities (policies and procedures)
+
System Integrator
integration capabilities
(design and deployment)
Automation Solution
Basic Process Control System (BPCS)
Safety Instrumented System (SIS)
Complementary hardware and software
IACS environment / project specific
Includes a configured instance of the Control System Product
Product Supplier
develops
Control System Product as a combination of
Supporting Applications
Embedded devices
Network components
Host devices
Independent of IACS environment
IEC

Figure 2 – Scope of service provider capabilities

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

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

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

NOTE ~~5~~ 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.

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.

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.

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.

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.

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

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.

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.

4.1.4 Profiles

~~Profiles are capability sets defined by selecting a specific subset of the requirements in Annex A. Profiles are intended to be written for different industry groups/sectors and other organizations to define one or more capability sets most appropriate to their needs.~~

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.

~~IEC Technical Reports (TRs) can be created by industry groups/sectors or other organizations to define profiles.~~ 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 ~~existing~~ these profiles to specify the requirements that ~~they need for~~ apply to their Automation Solutions.

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.

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.

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. 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 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		

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 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).

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

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, ~~defining~~ trust boundaries that subdivide the Automation Solution into partitions referred to as “zones” by IEC 62443-3-2.

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.

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.

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

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

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.

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.

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

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 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 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 ~~standard~~ 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 ~~to prevent requirements for~~ in place of specific security technologies, such as specific encryption algorithms. ~~Instead, it is used to require instances of specified concepts (e.g. encryption) that are commonly accepted and used by both communities. For example, which encryption mechanism a service provider uses to meet such a requirement would depend on when this standard is applied.~~ 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.

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 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).

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 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.

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.

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.

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.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.01.04	BR	Solution staffing	Background checks	Service provider	No	The service provider shall have the capability to ensure that it assigns only service provider personnel to Automation Solution related activities who have successfully passed security-related background checks, where feasible, and to the extent allowed by applicable law.	The capabilities specified by this BR and its REs are used to protect the Automation Solution from being staffed with personnel whose trustworthiness may be questionable. While the background check cannot guarantee trustworthiness, it can identify personnel who have had trouble with their trustworthiness. Having this capability means that the service provider has an identifiable process for verifying the integrity of the service provider personnel it will assign to work on the Automation Solution. This requirement also recognizes that the ability to perform background checks is not always possible because of applicable laws or because of lack of support by local authorities and/or service organizations. For example, there may be countries that do not prohibit background checks, but that provide no support for conducting a background check, making it infeasible or impractical for the service provider to perform such a check. How and how often background checks are performed are left to the service provider. Examples of background checks include identity verification and criminal record checks.
SP.01.04	RE(1)	Solution staffing	Background checks	Subcontractor	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 successfully passed security-related background checks where feasible, and to the extent allowed by applicable law.	Having this capability means that the service provider has an identifiable process for verifying the integrity of the subcontractors, consultants, and representatives of the service provider who will be assigned to work on the Automation Solution. This requirement also recognizes that the ability to perform background checks is not always possible because of applicable laws or because of lack of support by local authorities and/or service organizations. For example, there may be countries that do not prohibit background checks, but that provide no support for conducting a background check, making it infeasible or impractical for the service provider to perform such a check. How and how often background checks are performed are left to the service provider. Examples of background checks include identity verification and criminal record checks. See ISO/IEC 27036-3 for additional supply chain organizational requirements.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.01.05	BR	Solution staffing	Personnel assignments	Security contact	No	The service provider shall have the capability to assign a security contact in its organization to the Automation Solution who is responsible and accountable for the following activities. 1) Acting as liaison with the asset owner, as appropriate, about the service provider's and the Automation Solution's adherence to the Part 2-4 requirements that are required by the asset owner. 2) Communicating the service provider's point-of-view on IACS security to the asset owner's staff. 3) Ensuring that tenders to the asset owner are aligned and in compliance with the Part 2-4 requirements specified as required by the asset owner and the service provider's internal IACS security requirements. 4) Communicating to the asset owner deviations from, or other issues not conforming with, the Part 2-4 requirements that are required by the asset owner. This includes deviations between these requirements and the service provider's internal requirements.	The capability specified by this BR is used to The capability specified by this BR is used to enhance security-related communication between the asset owner and the service provider to allow the service provider to be more responsive to Automation Solution security needs. Having this capability means that the service provider has an identifiable process for assigning a person to the Automation Solution who will be responsible for coordinating security related issues with the asset owner, such as deviations from the Part 2-4 and Part 3-3 requirements. Having a security contact provides the organizational vehicle for the asset owner to work with the service provider to address deviations from Part 2-4 capabilities and deviations of the control system used in the Automation Solution from Part 3-3 requirements (e.g. how to provide compensating mechanisms).

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.01.06	BR	Solution staffing	Personnel assignments	Security lead	No	The service provider shall have documented minimum IACS cyber-security qualifications for security lead positions and the capability to assign security leads to Automation Solutions who ~~have demonstrated expertise in IACS cybersecurity~~ meet these qualifications.	The capability specified by this BR is used to reduce errors in security decision making and implementation. Making poor choices or lacking the ability to properly implement security can unnecessarily expose the Automation Solution to security threats and/or compromises. Having this capability means that the service provider has documented the qualifications (expertise/ competencies) that it requires of personnel who lead cyber-security related activities and has an identifiable process for staffing each Automation Solution with personnel who ~~are sufficiently qualified to lead cyber-security related activities~~ have this expertise. Expertise may include IACS cyber-security experience, training and certifications, and in general, the service provider and asset owner will typically come to agreement on the cyber-security qualifications for personnel before staffing begins. The ~~term "demonstrated"~~ phrase "meet these qualifications" is used to indicate that the security leads assigned to the Automation Solution have ~~evidence that shows their~~ relevant experiences that confirm their compliance with these qualifications.
SP.01.07	BR	Solution staffing	Personnel assignments	Change	No	The service provider shall have the capability to notify the asset owner of changes in service provider, subcontractor, or consultant personnel who have access to the Automation Solution.	The capability specified by this BR is used to protect the Automation Solution against threats posed by service provider, subcontractor, and/or consultant personnel who no longer need access to the Automation Solution. Once notified of changes in personnel, the asset owner can update access authorizations accordingly (e.g. revoking badges, removing user accounts and associated access control lists). Having this capability means that the service provider has an identifiable process for notifying the asset owner of changes in service provider staffing. Timeliness of the notification and which personnel changes require notification are typical elements agreed to by the service provider and the asset owner. For example, service provider personnel who access the Automation Solution using temporary accounts may not be included since their temporary accounts will be removed when they are no longer needed.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.02.01	BR	Assurance	Solution components	Verification	Yes	The service provider shall have the capability to provide documentation that verifies that Automation Solution components identified by the asset owner (e.g. as result of a security assessment, threat analysis, and/or security testing) have adequate security for their level of risk.	The capability specified by this BR is used to provide confidence that components in the Automation Solution have security capabilities commensurate with their level of security risk. Having this capability means that the service provider has an identifiable process for confirming that Automation Solution components provide the appropriate level of security protections required by the asset owner. Security assessments and certifications, testing, and/or other methods may be used to provide this confirmation. Security testing refers to system or component testing whose primary objectives are to discover vulnerabilities and, conversely, to verify that specific attacks are handled as intended (e.g. mitigated, defeated, and/or diverted/quarantined). The success of security testing does not necessarily mean that the item under test is free from vulnerabilities. Examples of security tests include penetration tests, fuzz tests, robustness tests, and vulnerability scans. For related supply chain requirements, see IEC 62443-4-1, IEC 62443-4-2, and ISO 27036-3.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.02.02	BR	Assurance	Security tools and software	Technical description	Yes	The service provider shall have the capability to recommend security analysis tools (e.g. network scanning tools) for use with the Automation Solution and: 1) Provide instructions on how to use them, 2) Identify any known adverse effects they may have on the Automation Solution's performance, 3) Provide recommendations for how to avoid adverse effects.	The capabilities specified by this BR and its REs are used to ensure that the Automation Solution can be examined for security-related issues using asset owner approved tools. Security-related issues include the discovery of unauthorized devices on the network and/or unauthorized open ports on a device. Having this capability means that the service provider has an identifiable process for recommending one or more security analysis tools for the Automation Solution, along with information on potential problems their use may cause, and instructions for how to avoid these issues. This requirement directly implies that the service provider has to be aware of the potential problems a tool that it recommends might cause and report them to the asset owner along with recommendations for how to avoid them and how to use the tool effectively. Avoiding potential problems associated with the use of a tool may be accomplished by restricting configuration options, scheduling testing at opportune times, or by other means. For example, if it is known that a network scanning tool has the potential for overloading the network, then it might be configured to limit its impact on network traffic, or the network might be segmented to reduce the scope of overloads.
SP.02.02	RE(1)	Assurance	Security tools and software	Approval	No	The service provider shall have the capability ensure that it obtains approval from the asset owner prior to using security analysis tools (e.g. network scans) at the asset owner's site.	Having this capability means that the service provider has an identifiable process for coordinating the use of security analysis tools in the Automation Solution with the asset owner and receiving approval to use them. The BR for this RE requires the service provider to be able to inform the asset owner of potential adverse effects that these tools may have on the Automation Solution.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.02.02	RE(2)	Assurance	Security tools and software	Detection	No	The service provider shall have the capability to schedule and use security analysis tools to discover undocumented and/or unauthorized systems or vulnerabilities in the Automation Solution. This capability shall include the ability to use these tools in accordance with the asset owner's standard operating procedures.	Having this capability means that the service provider has an identifiable process for using tools to discover unauthorized devices connected to networks within the Automation Solution and other vulnerabilities, such as open ports that should not be open. Having this capability also means that the service provider has an identifiable process for coordinating and scheduling the use of security analysis tools to prevent them from impacting operations of the Automation Solution. The BR for this RE requires the service provider to inform the asset owner of potential adverse effects that these tools may have on the Automation Solution. Integration service providers are encouraged to schedule the use of these tools just prior to handover, for example, to find unauthorized devices and open ports, while maintenance service providers should use them regularly according to asset owner defined cycles. NOTE Where applicable, the network scans should look for devices on both wired and wireless network segments in the Automation Solution.
SP.02.02	RE(3)	Assurance	Security tools and software	Robustness	No	The service provider shall have the capability to ensure the control system components used in the Automation Solution have the ability to maintain operation of essential control system functions in the presence of system and/or network scans during normal operation.	Having this capability means that the service provider has an identifiable process for ensuring that the components of the Automation Solution's control system accessible by network scanning tools are capable of withstanding network scans. See IEC 62443-3-3 for the system capabilities related to network scans. Robustness testing is often used to demonstrate this assurance.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.02.03	BR	Assurance	Hardening guidelines	Technical description	Yes	The service provider shall have the capability to provide documentation to the asset owner that describes how to harden the Automation Solution.	The capabilities specified by this BR and its RE are used to provide the asset owner with details of the security mechanisms and configuration settings for the Automation Solution. This supports asset owner initiatives to provide governance and detailed knowledge of Automation Solution security, including integration of the Automation Solution with plant networks and systems. Having this capability means that the service provider has an identifiable process for delivering a hardening guide that describes how to harden the Automation Solution (install/configure the security features of the Automation Solution). This hardening guide is to include both architectural and configuration considerations, such as firewall placement (architectural) and firewall rules (configuration) and also considerations when installing new components into the Automation Solution. In general, the hardening of the Automation Solution will follow recommendations of a risk assessment performed on the Automation Solution (see SP.03.01.BR and its REs). NOTE Hardening guides provided by the suppliers of the control system and other components used in the Automation Solution may be included in or referenced by the service provider's hardening guide.
SP.02.03	RE(1)	Assurance	Hardening guidelines	Verification	No	The service provider shall have the capability to verify that its security hardening guidelines and procedures are followed during Automation Solution related activities.	Having this capability means that the service provider has an identifiable process for ensuring that personnel and their subcontractors/consultants/representatives follow the hardening procedures required in SP.02.03 BR. Checklists are often used for this purpose.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.01	BR	Architecture	Risk assessment	Perform	No	The service provider shall have the capability to conduct a security risk assessment of the Automation Solution or contribute to (participate in) a security risk assessment conducted by the asset owner or its agent. NOTE 1 The asset owner may additionally require the service provider to document its assessment. The “Doc?” column is set to “No” because this is a requirement to have the capability to perform the assessment and not a requirement to provide documentation.	The capabilities specified by this BR and its REs are used to ensure that the service provider is capable of identifying and analyzing risks to support identification and remediation of security risks to the Automation Solution. Having this capability means that the service provider has an identifiable process for performing or contributing to a risk assessment. In some cases, the asset owner will require the service provider to conduct the assessment, while in other cases, to take an active role in an assessment conducted by the asset owner or by a third party under the direction of the asset owner. In an active role, the service provider might be asked to provide detailed knowledge of the Automation Solution and its components, information about threats and/or vulnerabilities, or otherwise assist in an assessment that has significant participation/contribution by the asset owner. For guidance on perfuming risk assessments, see IEC 62443-2-1 and IEC 62443-3-2. NOTE 2 Security risk assessments can be performed at any point in Automation Solution design and implementation to identify and manage security risks, but are often first performed prior to Automation Solution design to provide the basis for security design decisions, and then often repeated to ensure that security risks are kept current. NOTE 3 Risk assessment performed at the time of commissioning provides the asset owner a benchmark based on the achieved or as-built security system. NOTE 4 The output of the security risk assessment is a contractual matter between the service provider and the asset owner.
SP.03.01	RE(1)	Architecture	Risk assessment	Reporting	No	The service provider shall inform the asset owner of the results of security risk assessments that it performs on the Automation Solution, including risk mitigation mechanisms and procedures.	Having this capability means that the service provider has an identifiable process for reviewing risk assessments of the Automation Solution which it has performed and for informing the asset owner of security issues that were found, including recommendations for security mechanisms/procedures to address them.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.01	RE(2)	Architecture	Risk assessment	Verification	No	The service provider shall have the capability to verify that security architecture reviews and/or security assessment and/or threat analysis of the control system used in the Automation Solution have been conducted by a third party.	Having this capability means that the service provider can provide verification that the security of the control system used in the Automation Solution has been reviewed by a third party. Typically the review is done on the control system product under the direction of the control system supplier.
SP.03.02	BR	Architecture	Network design	Connectivity	No	The service provider shall have the capability to ensure that the physical network segmentation architecture used in the Automation Solution, including its use of network security devices or equivalent mechanisms, is implemented according to the Automation Solution design approved by the asset owner.	The capabilities specified by this BR and its REs are used to ensure the use of access controls between network segments within the Automation Solution and between the Automation Solution and external networks/communication links. Access controls protect network segments by restricting traffic flows between them. Restrictions are generally defined by rules that whitelist and/or blacklist traffic based on a number of factors including source addresses, destination addresses, and content (e.g. deep packet inspection). Having this capability means that the service provider has an identifiable process for ensuring that the Automation Solution networks have been segmented as specified and as approved by the asset owner. The location of the network segmentation points and their corresponding network security devices should be based on a risk assessment (see IEC 62443-3-2) and on the requirements in this standard (IEC 62443-2-4). As implementation progresses, having this capability also means that the service provider has an identifiable process for ensuring that design documents are updated so that they accurately reflect the Automation Solution architecture (see SP.06.01 BR).
SP.03.02	RE(1)	Architecture	Network design	Connectivity	No	The service provider shall have the capability to identify and document the network segments of the Automation Solution and their interfaces to other segments, including external networks, and for each interface designate whether it is trusted or untrusted.	Having this capability means that the service provider has an identifiable process for identifying all network segments of the Automation Solution, how they are interconnected, which of them provide external access to the Automation Solution, and for designating each connection point (interface to/from a segment) as trusted or untrusted. Untrusted interfaces are those that allow connections with untrusted devices in other segments/systems. Risk assessments as described in IEC 62443-3-2 can be used in the determination of trust and the use of zones to establish trust boundaries.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.02	RE(2)	Architecture	Network design	Connectivity	No	The service provider shall have the capability to ensure that interfaces of the Automation Solution that have been identified as untrusted are protected by network security devices or equivalent mechanisms, with documented and maintained security rules. At a minimum, the following shall be protected: 1) External interfaces 2) Level 2/Level 3 interfaces (see NOTE 2 below) 3) Interfaces between the BPCS and the SIS 4) Interfaces connecting wired and wireless BPCS networks 5) Interfaces connecting the BPCS to data warehouses (e.g. enterprise historians) NOTE 1 For some, responsibility for maintaining firewall rules and documentation transfers to the asset owner prior to or at Automation Solution turnover. In this case, the service provider's role may be, as required by the asset owner, only to support verification that the firewall rules are accurate and up-to-date. NOTE 2 Depending on the Automation Solution, Level 2/Level 3 interfaces may be "External" interface.	Having this capability means that the service provider has an identifiable process for protecting the Automation Solution from external access and for controlling access between Level 2 ~~from~~ and Level 3 (e.g. through the use of firewalls/firewall rules). Within the Automation Solution, having this capability also means that the service provider has an identifiable process for protecting BPCS interfaces using network security devices or equivalent mechanisms, and for providing the information necessary to create security rules that are used to grant/deny access to BPCS ports and applications. If the service provider supplies or is responsible for the network security device or the equivalent mechanism, then the required support includes being able to configure the network security device/mechanism as needed. Risk assessments (see IEC 62443-3-2) can be used to determine which interfaces require safeguarding.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.03	BR	Architecture	Solution components	Vulnerabilities	No	The service provider shall have capabilities for handling vulnerabilities that affect the Automation Solution, including its related policies and procedures. These capabilities shall address: 1) The handling of vulnerabilities newly discovered in the Automation Solution or in its related policies and procedures for which the service provider is responsible, and 2) The handling of publically disclosed vulnerabilities affecting the Automation Solution.	Having this capability means that the service provider has an identifiable process for assessing, reporting, and disposing of (e.g. recommending mitigations, preparing remediation plans) vulnerabilities related to the Automation Solution components for which the service provider is responsible. Typically, the process of identifying vulnerabilities includes event analysis and correlation (see SP.08.01 BR), risk assessment (see SP.03.01 BR and its REs), network scans and other automated methods (see SP.02.02 BR and its REs), and assurance (see SP.02.01 BR). Software patches that result from the disposition of vulnerabilities are considered to be security patches.
SP.03.03	RE(1)	Architecture	Network design	Vulnerabilities	Yes	The service provider shall have the capability to provide documentation to the asset owner that describes how to mitigate security weaknesses inherent in the design and/or implementation of communication protocols used in the Automation Solution that were known prior to Automation Solution integration or maintenance activities.	The capability specified by this BR is used to ensure that compensating mechanisms are used to address weaknesses in Automation Solution communications. Having this capability means that the service provider has an identifiable process for informing the asset owner about known communication weaknesses in the Automation Solution and how to mitigate them. For example, if the Automation Solution uses unencrypted protocols for the transfer of sensitive data, then the service provider should recommend security measures, such as lockable switches and physical security for communication links, to protect transmission of the data. NOTE The asset owner may also require the service provider, as part of its service agreement with the service provider or via a separate service agreement, to inform the asset owner of the discovery of additional weaknesses/mitigations discovered after the normal term of integration or maintenance activities.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.04	BR	Architecture	Network design	Network time	No	The service provider shall have the capability to ensure that time distribution/synchronization for the Automation Solution is performed from a secure and accurate source that uses a protocol that is commonly accepted by both the security and industrial automation communities.	The capability specified by this BR is used to ensure that timestamps are used in the Automation Solution and that they are generated and distributed from a reliable source. Timestamps are used in forensics when examining event logs. Having this capability means that the service provider has an identifiable process for integrating a network time source into the Automation Solution. The ability to provide the time source is not within the scope of this requirement. However, whether or not the service provider provides the time source, it is the responsibility of the service provider to integrate the time source into the Automation Solution. An example of a commonly accepted time source protocol IEEE 1588-2008/IEC 61588:2009.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.05	BR	Architecture	Devices – All	Least functionality	No	The service provider shall have the capability to ensure that only software and hardware features required by the Automation Solution or approved by the asset owner are enabled in the Automation Solution. At a minimum, this includes ensuring that: 1) unnecessary software applications and services (e.g. email, office applications, games) and their associated communication access points (e.g. TCP/.UDP ports), USB devices (e.g. mass storage), Bluetooth and wireless communications are disabled and/or removed unless required by the Automation Solution. 2) network addresses in use are authorized, 3) physical and logical access to diagnostic and configuration ports is protected from unauthorized access and use. 4) unused ports on network devices (e.g. switches and routers) are configured to prevent unauthorized access to the Automation Solution's network infrastructure. 5) maintenance processes maintain the hardened state of the Automation Solution during its lifetime.	The capabilities specified by this BR and its RE are used to limit access to the Automation Solution by removing/disabling unnecessary features and preventing unauthorized access to different types of Automation Solution interfaces (e.g. network device and configuration/diagnostic ports). Having this capability means that the service provider has an identifiable process for reducing the attack surface of the Automation Solution, for limiting access to the listed interfaces/ports to authorized users, and for maintaining the hardened state of the Automation Solution. This process may include the use of network security tools described in SP.02.02 BR and its REs. Limiting the software applications and their associated communication access points, USB devices such as mass storage devices, and wireless communications capabilities to only those necessary to perform the functions of a device used in both normal and emergency operations reduces the number of avenues into the device for an attack. Identifying unnecessary and/or unauthorized access points (e.g. using network scanning tools) is one technique that can be used to discover unnecessary software programs. Identifying network addresses that are unauthorized, for example using network scans as described in SP.02.02 RE(2), and removing them (e.g. by disconnecting the devices to which they are assigned) limits the source of passive and active attacks. Controlling access to physical configuration ports of devices, such as serial ports is intended to prevent or reduce the risk of having the network configuration (network devices) or the operation of other devices changed without proper authorization. Different methods for controlling access include installing a device in a locked cabinet, being able to physically lock the configuration port, or otherwise disabling use of the port when its use is not authorized (e.g. through a software lock).

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
							Locking down network device ports (switches and routers) reduces the possibility that an unauthorized device will be able to connect to the network and launch attacks or sniff the network. Control system products may have already removed capabilities unused by them prior to or during installation, making it necessary for the service provider to ensure that they are added/enabled only if they are required and approved by the asset owner. Maintenance processes provide the possibility that previously hardened components of the Automation Solution are reset or reconfigured to lose some aspect of their hardening. Controlling these processes reduce this possibility.
SP.03.05	RE(1)	Architecture	Devices – All	Least functionality	No	The service provider's hardening guidelines and procedures shall ensure that only necessary, authorized, and documented digital certificates for certificate authorities (CAs) are installed.	Having this capability means that the service provider has an identifiable process for determining which CA certificates are installed and removing those that are not used/authorized. Typically operating system installation and upgrades cause a generic set of Certificate Authority certificates to be installed, even though they are not required for the Automation Solution. Limiting which CA certificates are installed to only those that are necessary prevents authentication of unwanted, undesirable, or unnecessary applications.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.06	BR	Architecture	Devices – Workstations	Session lock	No	The service provider shall have the capability to support the use of session locking for Automation Solution workstations as required by the asset owner. This requirement applies only to the workstations for which the service provider is responsible. Session locking: 1) prevents information on the logged on user's display device from being viewed, and 2) blocks input from the user's input device (e.g. keyboard, mouse) until unlocked by the session user or an administrator. NOTE Locking the user input device means that the user at the workstation is not able to use the keyboard except for unlocking the keyboard.	The capability specified by this BR is used to ensure that workstations can be locked to protect against disclosure of information on the user's display device (e.g. screen) and against use of the user input device (e.g. keyboard, mouse). Having this capability means that the service provider has an identifiable process for enabling automatic screen locking for workstations, as required by the asset owner. Automatic screen locking causes the workstation screen to stop displaying and prevents data input until the authorized logged-on user unlocks the screen, typically by reentering the password. Which workstations need automatic screen locking enabled is defined by the site security requirements, which are often the result of a risk assessment (see IEC 62443-3-2). For example, workstations used to administer network devices and wireless networks are normally unattended and in accessible locations and therefore require automatic session locking enabled. This requirement only applies to workstations for which the service provider is responsible.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.07	BR	Architecture	Devices – Workstations	Access control	No	The service provider shall have the capability to ensure that wired and wireless workstations, including handhelds, used for maintenance and engineering of wired and wireless control/instrumentation devices do not circumvent the: 1) Automation Solution’s access controls for these devices, 2) network security safeguards (e.g. network security devices) at the Automation Solution's boundary with Level 3. NOTE 1 Direct access to these devices by handhelds that bypass access controls of the Automation Solution is prohibited. NOTE 2 Direct access by a handheld to a wireless device in Level 3 that bypasses the Level 2/3 network security device is prohibited.	The capabilities specified by this BR and its RE are used to ensure that the Automation Solution’s access controls (including authentication mechanisms) are always used to prevent unauthorized access to the Automation Solution’s field devices from workstations/handhelds. Having this capability means that the service provider has an identifiable process for ensuring that there are no direct paths between workstations/handhelds and control/instrumentation devices that bypass the control system's access controls. The assumption is that access controls to these devices by engineers and operators is built into the control system. However, maintenance or engineering may be done using handhelds or other workstations that are not tightly integrated with the control system, and this required capability ensures that they cannot directly connect to control/instrumentation devices, bypassing the control system's access controls.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.07	RE(1)	Architecture	Devices – Workstations	Access control	No	The service provider shall have the capability to support the use of multi-factor authentication for Automation Solution workstations as required by the asset owner. This requirement applies only to the workstations for which the service provider is responsible.	Having this capability means that the service provider has an identifiable process for using multi-factor authentication in workstations as required by the asset owner. This support may include the ability to supply the necessary hardware and/or set up workstations to enforce multi-factor authentication. In practice, the type and level of authentication used for workstations will be defined by the site security requirements, which are often the result of a risk assessment (see IEC 62443-3-2). In general, multi-factor authentication is used for workstations that are accessible by personnel who are not authorized users of the Automation Solution, such as workstations that are normally unattended and/or in uncontrolled spaces. This requirement only applies to workstations for which the service provider is responsible. Multi-factor authentication includes, at a minimum, at least two of the following: 1) something the user knows, such as a password, 2) something the user possesses (a physical token), such as a smart card, 3) something inherent about the user, such as a retinal scan 4) someplace you are.
SP.03.08	BR	Architecture	Devices – Network	Least functionality	No	The service provider shall have the capability to ensure that least privilege is used for the administration of network devices for which the service provider is responsible.	This BR and its REs recognize that network devices are critical to the Automation Solution, and as a result, are often the subject of attack. Therefore, this BR and its REs are defined to ensure that the various facets of network device administration are protected. Having this capability means that the service provider has an identifiable process for applying the concept of least privilege to the administration of network devices. Least privilege for administrative operations means that access is granted only to resources (e.g. directories and files) that are needed and operating system privileges are similarly restricted to only those that are needed.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.08	RE(1)	Architecture	Devices – Network	Access control	No	The service provider shall have the capability to ensure that access controls used for the administration of network devices and wireless networks include role-based access controls. NOTE Normally network devices are only accessed by administrators so it is necessary to define only a single role for them. However, if the asset owner’s operating procedures allow access to the network devices by administrators and others, then multiple roles can be defined.	Having this capability means that the service provider has an identifiable process for configuring network devices to use role-based access controls. Defining separate roles allows separate access control lists to be defined for each role, thus supporting the concept of least privilege. Normally, network devices are accessed only by administrators so only one role needs to be defined and the access control list to be set accordingly. However, if the asset owner's operating procedures provide for different levels of network device administration, then multiple roles need to be defined. Users capable of administering network devices will then be granted these roles. See IEC 62351-8 for further discussion of role based access controls.
SP.03.08	RE(2)	Architecture	Devices – Network	Cryptography	No	The service provider shall have the capability to ensure that encryption is used to protect data, whether in transit or at rest, that is used in the administration of network device (e.g. passwords, configuration data) that is identified as data requiring safeguarding (see SP.03.10 BR and its REs). NOTE See SP.03.10 RE(3) for cryptographic requirements.	Having this capability means that the service provider has an identifiable process for ensuring that data used for the administration of network device that is regarded as sensitive data as specified in SP.03.10 BR and its REs is protected by encryption within the device and on communication links. Encryption used on communications links can be performed at the network layer, on the transport layer connection, or at the message level to protect the data “on the wire”. Encryption within network devices is used to prevent attacks on the configuration by malicious software in the device (e.g. as a result of hacking). The use of encryption mechanisms that provide integrity protection should be considered, such as AES_GCM.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.08	RE(3)	Architecture	Devices – Network	Access control	No	The service provider shall have the capability to ensure that access controls used for the administration of network devices include mutual authentication.	Having this capability means that the service provider has an identifiable process for configuring network devices to use mutual authentication. Mutual authentication validates the identity of the user and the network device, and results in the ability of the network device to determine whether the user is authorized to access the device, and in the ability for the user to ensure the device is the intended device and is not being spoofed. Challenge/response, user password/device certificate, and Kerberos (RFC 1510), are examples of techniques used to provide mutual authentication.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.09	BR	Architecture	Data protection	Communications	No	The service provider shall have the capability to ensure that the Automation Solution is configured to verify that all control actions and data flows in the Automation Solution (e.g. between workstations and controllers), including configuration changes, are: 1) valid, 2) initiated or approved by an authorized user, and 3) transferred over an approved connection in the approved direction.	The capability specified by this BR is used to ensure that there are manual and/or automated controls in place to prevent Automation Solution devices, such as controllers, from executing invalid and/or unauthorized commands. Having this capability means that the service provider has an identifiable process for ensuring that all commands (e.g. writes to setpoints, configuration commands) sent to Automation Solution devices (e.g. from workstations) are valid (within authorized limits), are authorized by a user with the appropriate permissions, and are transferred to the device executing the command (e.g. controller) over a connection that has been designated/authorized to be used for this purpose (e.g. a connection from an Operator Console to a controller). The intent of the second item of the requirement is to make sure that commands can only be requested by authorized users (e.g. operators), that the entity receiving and executing the command knows which connections are authorized for receiving commands, and that the command is checked for validity. Validity is normally value and state dependent. For example, a setpoint normally is not allowed to be written by the operator without putting the loop into manual control. This requirement also requires the service provider to have an identifiable process for ensuring that data flows are conducted over an authorized connection and that the data is transferred in the authorized direction. The intent of this portion of the requirement is make sure that the flow of data, including the direction, is authorized and conducted over authorized connections. For example, if a dynamic change (not a configuration change) to a set point is initiated by an entity not explicitly authorized to make the change, such as an advanced control application, then the system will notify the operator of the change and the operator is required to approve it before it can take effect. If the operator does not approve it, the set point does not change.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
							NOTE 1 This requirement generally applies to commands issued by workstations and sent to controllers, and not to commands sent from controllers to Level 1 devices. NOTE 2 Authorization of connections may be performed automatically by the control system and/or through appropriate configuration by the service provider (setting up network addresses/ports authorized to send commands. NOTE 3 Risk assessments (see IEC 62443-3-2) can be used to determine which connections are authorized to perform control actions. If warranted by the risk assessment, "dual approval" system capabilities (see IEC 62443-3-3) can be used to support this requirement. Dual approval refers to the system requiring two people to authorize actions that can result in serious impact to the iACS. NOTE 4 "Initiated or approved by" means, for example, that the Automation Solution can prevent remote operators from changing setpoints without approval by the local operator through the authorized connection. How this is implemented is Automation Solution dependent.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.10	BR	Architecture	Data protection	Sensitive data	Yes	The service provider shall have the capability to ensure that data storage points and data flows within the Automation Solution that require safeguarding, as defined or approved by the asset owner, are documented, including the security requirements for their safeguarding (e.g. confidentiality, integrity).	The capabilities specified by this BR and its REs are used to ensure that data stored and/or transferred in the Automation Solution that needs protection is documented and adequately protected. Typically both the asset owner and the service provider collaborate to identify control system data that needs protection (e.g. passwords, certificates, keys) and other data deemed worthy of protection by the asset owner (e.g. recipes). Having this capability means that the service provider has an identifiable process for identifying the data within the Automation Solution, either at rest or in transit, that requires protection and the type of protection required. The definition of data requiring safeguarding often contains site-specific criteria, and therefore, the asset owner should provide or at least approve the criteria. Data at rest can be in memory or in a storage device, and data in transit is data that is being transferred from one entity to another (a data flow). Examples of the types of data to be protected include (this list is not exhaustive): 1) legal or regulatory information 2) asset owner confidential data, including proprietary data (e.g. recipes) and data identified in NDAs or other contractual vehicles 3) configuration and operational data (e.g. commands and parameters) 4) system data, such as cryptographic materials (e.g. keys and certificates), access control lists, passwords, network device data, 5) audit and event logs, 6) backup data, 7) historical data, 8) data warehouses.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.10	RE(1)	Architecture	Data protection	Sensitive data	No	The service provider shall have the capability to ensure that data within the Automation Solution requiring safeguarding, as described in SP 03.10 BR, is protected from unauthorized disclosure or modification, whether at rest or in transit.	Having this capability means that the service provider has an identifiable process for ensuring that, after the sensitive data in an Automation Solution has been identified, the Automation Solution is enhanced as necessary to protect that data. Risk assessments (see IEC 62443-3-2) performed early in the project are often used in the identification of data requiring safeguarding. Protection mechanisms typically include: 1) mechanisms to protect against unauthorized memory dumps and network sniffing, 2) cryptographic mechanisms, including: a) encryption keys b) public key security infrastructure, c) digital signatures, d) data transport and message encryption, e) data base encryption.
SP.03.10	RE(2)	Architecture	Data protection	Data/event retention	Yes	The service provider shall have the capability to provide documentation to the asset owner that describes the retention capabilities provided by the Automation Solution for storing/archiving sensitive data. This documentation includes capacities, pruning and purging functions, retention timeouts, etc.	Having this capability means that the service provider has an identifiable process for documenting how the Automation Solution stores/archives sensitive data, such as historical data and events. This may include internal capabilities of the Automation Solution ~~or that it requires export~~ (e.g. data volumes/capacities) or may identify capabilities required to export historical data/events to a history archive. Historical data and events can be used during forensics and event analysis and correlation.
SP.03.10	RE(3)	Architecture	Data protection	Cryptography	No	The service provider shall have the capability to ensure that the cryptographic mechanisms used in the Automation Solution, including algorithms and key management/distribution/protection, are commonly accepted by both the security and industrial automation communities.	Having this capability means that the service provider is able to ensure that components of the Automation Solution that it provides uses current encryption technology that is generally accepted for use in IACSs.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.10	RE(4)	Architecture	Data protection	Sanitizing	No	The service provider shall have the capability to ensure that when it removes a component from the Automation Solution, all data in the component requiring safeguarding, as described in SP 03.10 BR, is permanently destroyed/deleted.	The capability specified by this BR is used to prevent sensitive data in a component/device that has been removed from the Automation Solution from being subsequently disclosed to anyone who may have access to the component after its removal. Having this capability means that the service provider has an identifiable process for ensuring that devices that are removed from active participation in the Automation Solution are sanitized of their confidential or sensitive data. Typically this can be done by destroying memory or clearing it a number of times to remove residual data. The number of times memory has to be cleared is dependent on the type of memory.
SP.04.01	BR	Wireless	Network design	Technical description	No	The service provider shall have the capability to ensure that its Automation Solution architecture documentation describing wireless systems is current in its description of the following. 1) Data exchange between a Level 1 network and wireless instrumentation, 2) Data exchange between a Level 2 network and a Level 3 network through a secure wireless link, 3) Security mechanisms that prevent an intruder from gaining access to the Automation Solution using the wireless system, 4) Security mechanisms that restrict access within the Automation Solution by workers with handheld wireless devices, 5) Where required, security mechanisms that provide protection for remote management of wireless systems. NOTE 1 The term "Level" refers to the position in the Purdue Reference Model as standardized by ISA 95 and IEC 62264-1 (see clause 5.3).	The capability specified by this BR is used to ensure that wireless networks are protected from being used to gain unauthorized access to the Automation Solution. Having this capability means that the service provider has an identifiable process for keeping current its wireless communications architecture documentation that includes data flows, security mechanisms, and the use of wireless bridges. NOTE 2 Zones and conduits as described in IEC 62443-3-2 are often used to define the security boundaries associated with wireless access to wired devices/workstations in the Automation Solution.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.04.02	BR	Wireless	Network design	Access control	No	The service provider shall have the capability to ensure that access to wireless devices is protected by authentication and access control mechanisms that are commonly accepted by both the security and industrial automation communities.	The capabilities specified by this BR and its RE are used to ensure that wireless devices and their communications are protected from unauthorized access. Having this capability means that the service provider has an identifiable process for providing or using commonly accepted authentication mechanisms and access control lists that prevent unauthorized access to wireless devices.
SP.04.02	RE(1)	Wireless	Network design	Communications	No	The service provider shall have the capability to ensure that wireless communications are protected by cryptographic mechanisms that are commonly accepted by both the security and industrial automation communities.	Having this capability means that the service provider has an identifiable process ensuring that networks used in the Automation Solution employ commonly accepted security mechanisms to protect access to their data during transmission. This includes wireless communications between wireless devices and wireless access points and between wireless access points and other wireless access point.
SP.04.03	BR	Wireless	Network design	Communications	No	The service provider shall have the capability to ensure that wireless protocols used in the Automation Solution are compliant with standards commonly used within the industrial security community and with applicable regulations.	The capabilities specified by this BR and its REs are used to provide confidence that wireless networks use protocols that have been vetted for use in industrial applications. Having this capability means that the service provider (1) uses a commonly accepted standard wireless technology in the Automation Solution and (2) has an identifiable process that ensures that the wireless technology used is compliant with local regulations.
SP.04.03	RE(1)	Wireless	Network design	Wireless network identifiers	No	The service provider shall have the capability to ensure that unique, Automation Solution-specific identifiers are used for wireless networks and that all wireless identifiers are descriptive acronyms that are not obviously associated with the asset owner's site.	The capability specified by this RE is used to provide confidence that wireless networks are configured to prevent easy identification (network identifiers are not obvious). Having this capability means that the service provider has an identifiable process for ensuring that each wireless network is assigned its own identifier (e.g. SSID) and that these identifiers do not allow an external listener to identify the physical wireless network, its location, or owner of the wireless network. If the identifier values are defined by the asset owner, the service provider's role is, if required, to provide guidance for their definition and/or review of the defined identifiers.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.04.03	RE(2)	Wireless	Network design	Connectivity	No	The service provider shall ensure that the Automation Solution's wireless devices that have IP addresses use static addressing and have dynamic address assignment mechanisms (e.g. DHCP) disabled.	The capability specified by this RE is used to provide confidence that wireless networks are configured to prevent: 1) the use of unauthorized device addresses, 2) DHCP exhaustion attacks (by disabling the use of DHCP). Having this capability means that the service provider has an identifiable process for ensuring that wireless device that have IP addresses cannot have their addresses changed by dynamic address assignment mechanisms.
SP.05.01	BR	SIS	Risk assessment	Verification	No	The service provider shall have the capability to verify that security architecture reviews and/or security risk assessments of the communications of the SIS used in the Automation Solution have been conducted and addressed.	The capability specified by this BR is used to provide confidence that security risks associated with the SiS are addressed. Having this capability means that the service provider can provide verification that the security of SIS communications, both internal and external, identified by risk assessments/security reviews have been addressed. Typically the review is done on integrated SIS/control system product under the direction of the control system supplier in response to IEC 61511-1 Clause 8.2.4, and addressed by the supplier. In some cases, mitigation of risks is deferred to the service provider as part of the installation/maintenance of the Automation Solution. In these cases, this requirement requires the service provider to ensure the appropriate mitigations for the Automation Solution are determined and implemented.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.05.02	BR	SIS	Network design	Communications	No	The service provider shall have the capability to ensure that SIS safety ~~critical~~ communications and SIS safety functions are protected from the BPCS or any other Automation Solution communications ~~are physically or logically separated and that any failures at the interface between them do not impact the SIS from performing its safety functions~~. NOTE This requirement does not require that ~~non-safety critical~~ communications not critical to safety functions between the SIS and the BPCS (e.g. configuration downloads, status monitoring, logging) be ~~separated~~ shielded from other Automation Solution communications.	The capability specified by this BR is used to ensure that ~~safety-critical communications of the SIS is not subject to interference by non-safety critica communications~~ SIS communications critical to safety functions cannot be affected by other communications of the Automation Solution. Having this capability means that the service provider is able to ~~logically or physically isolate functional safety~~ protect or isolate SIS communications critical to safety functions from other Automation Solution traffic ~~for SIL 1 and above~~ (see IEC 61508), for example, through the physical separation of BPCS communications and the SIS. In this example, firewalls and non-routable interfaces between the BPCS and SIS could be used to enforce this separation. Having this capability also means the service provider can demonstrate that the countermeasures taken to isolate functional safety communications do not impact the performance or operation of ~~the SIS~~ communications critical to safety. Risk assessments, zones (network segments), and conduits (connections between network segments), as described in IEC 62443-3-2, can be used in the definition of requirements.
SP.05.03	BR	SIS	Network design	Communications	No	The service provider shall have the capability to ensure that ~~applications, including remote access applications (e.g. RDP) at Level 3 and above are not able to establish (or otherwise have) connections with the SIS~~ communications external to the Automation Solution, including remote access communications, are not able to interfere with the operation of the SIS. ~~NOTE The term "Level" refers to the position in the Purdue Reference Model as standardized by ISA 95 and IEC 62264-1 (see 5.3).~~	The capability specified by this BR is used to ensure that the ~~SIS is not capable of being impacted by devices/applications in Level 3~~ operation of the SIS cannot be impacted by communications of devices/applications external to the Automation Solution. SP.05.02 BR requires capabilities to protect SIS communications from other Automation Solution communications, while this requirement requires capabilities to protect the operation of the SIS from communications external to the Automation Solution. Having this capability means that the service provider has an identifiable process for ensuring that the operation of the SIS cannot be ~~connected, physically or logically, to Level 3 or above~~ affected by communications of external applications, including remote access communications such as RDP. ~~Applications above Level 2 are not allowed to connect directly to the SIS.~~

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.05.04	BR	SIS	Network design	Communications	No	The service provider shall have the capability to ensure that ~~there are no safety-critical communications between the SIS and applications outside the SIS (e.g. control system applications)~~ applications, (e.g. control system applications) external to the SIS are not able to participate in or disrupt or otherwise interfere with SIS communications that are critical to safety functions.	The capability specified by this BR is used to ensure that ~~a trust boundary is established between the SIS and the BPCS that does not permit SIS safety critical communications to cross the trust boundary~~ the SIS cannot be impacted by devices/applications external to the SIS. SP.05.03 BR requires capabilities to protect the SIS from communications external to the Automation Solution, while this requirement requires capabilities to protect SIS communications from interference by applications external to the SIS. Having this capability means that the service provider has an identifiable process for ensuring that there are no ~~safety-critical~~ communications critical to safety functions (e.g. data and/or commands) transferred between the SIS and applications residing external to the SIS. This requirement is intended to prevent the SIS ~~safety-critical~~ functions critical to safety operations from being compromised by traffic originating from sources outside the SIS.
SP.05.05	BR	SIS	Devices – Workstations	Communications	No	The service provider shall have the capability to ensure that ~~all communications from Level 3 and above to~~ SIS EWSs that reside outside the SIS ~~pass through a network security device, or equivalent mechanism, that separates Level 2~~ (external to SIS interface with the control system) cannot be compromised by communications from Level 3 or above. NOTE The term "Level" refers to the position in the Purdue Reference Model as standardized by ISA 95 and IEC 62264-1 (see 5.3).	The capability specified by this BR is used to ~~be able to use~~ employ safeguards, such as network security devices, to ensure that only authorized communications from Level 3 applications to SIS engineering workstations residing outside the SIS are permitted. Access from Level 3 applications to SIS engineering workstations that reside within the SIS is prohibited by SP.05.03 BR. Having this capability means that the service provider has an identifiable process for ensuring that all communications between the SIS engineering workstation and Level 3 (and above) applications pass through a network security device, or equivalent mechanism, that connects Level 2 and Level 3 (or above).

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.05.05	RE(1)	SIS	Devices – Workstations	Communications	No	The service provider shall have the capability to ensure that ~~remote access (e.g. RDP) to~~ the Automation Solution's SIS EWS ~~is not possible~~ that reside within the SIS (internal to SIS interface with the control system) cannot be compromised by remote access (e.g. RDP).	The capability specified by this RE is defined to be able to ~~prevent~~ protect SIS engineering workstations that reside inside the SIS from being exploited via remote access connections. See SP.05.05 BR that addresses access from Level 3 to SIS EWSs external to the SIS. Having this capability means that the service provider has an identifiable process for ensuring that SIS engineering workstations within the SIS (1a) either ~~(1)~~ do not have remote access installed or (~~2~~ 1b) have it disabled (not accessible), and/or (2) have security mechanisms that block remote access communications with these workstations. ~~A risk assessment can be used to determine the risk of allowing remote access to the SIS EWS.~~ NOTE See IEC 62443-3-2 for guidance on what to consider in such risk assessments from a cyber-security perspective.
SP.05.06	BR	SIS	Devices – Workstations	Connectivity	No	The service provider shall have the capability to ensure that all access to the Automation Solution's SIS from outside the SIS is mediated and authorized at the interface to the SIS. ~~1) via a Level 2 gateway dedicated to the SIS and physically connected to it (e.g. via a dedicated link), and/or~~ ~~2) from a SIS EWS that is physically connected to the SIS. If the SIS EWS is not physically connected to the SIS, then its only option is to communicate to the SIS via the gateway described in (1).~~	The capability specified by this BR is used to limit the number of physical access paths to the SIS, and hence reduce its attack surface. Having this capability means that the service provider has an identifiable process for ensuring that ~~the SIS is physically connected only to~~ access controls to the SIS are implemented at the interface to the SIS, for example by a gateway used only to provide access to the SIS from the BPCS. Implementation of this gateway may be provided by the BPCS or the SIS. ~~1) the SIS EWS and/or~~ ~~2) a gateway used only to provide access to the SIS from Level 2.~~ ~~If the first case is not used then, the SIS EWS connects to the gateway and the gateway makes requests to the SIS on behalf of the SIS EWS.~~

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.05.07	BR	SIS	Devices – Workstations	Least functionality	No	The service provider shall have the capability to ensure that SIS functions performed by the Automation Solution's SIS EWS ~~is restricted to performing SIS functions~~ are protected from compromise by other SIS EWS software.	The capability specified by this BR is used to reduce the possibility that the SIS EWS will contain T3 offline software (see IEC 61508-3) that could intentionally or inadvertently cause harm to the SIS. Having this capability means that the service provider has an identifiable process for ensuring that ~~SIS engineering workstations are dedicated to SIS and are not used as workstations for other purposes within the control system~~ safety-related software running in SIS EWSs is protected from compromise from other software running in the SIS EWS.
SP.05.08	BR	SIS	Devices – Wireless	Connectivity	No	The service provider shall have the capability to verify that unauthorized wireless devices are not ~~allowed~~ used as an integral part of SIS safety functions.	The capability specified by this BR is used to prevent ~~wireless~~ attacks against the SIS by unauthorized wireless devices. Since wireless devices are not bounded by physical security perimeters nor by physical implementation, they can present a threat to the SIS. ~~For example, if a workstation/server class machine resides outside the physical security perimeter and is configured with a wireless device interface and is able to connect to the wireless device network, it will pose a threat to the SIS.~~ Having this capability means that the service provider has an identifiable process for verifying that wireless device communications are not used ~~within the SIS~~ as an integral part of SIS safety functions when prohibited by the asset owner. “Integral part” refers to communications that are implemented and incorporated into SIS safety functions. See SP.04.01 BR for requirements for the general use of wireless technologies within the Automation Solution.
SP.05.09	BR	SIS	User interface	Configuration mode	No	The service provider shall have the capability to ensure that ~~the Automation Solution provides a user interface for enabling and disabling SIS configuration mode~~ SIS configuration mode can be enabled and disabled. While ~~locked~~ disabled, this interface shall prohibit the SIS from being configured. NOTE This interface will typically prevent configuration messages from being delivered to the SIS.	The capabilities specified by this BR and its REs are used to prevent configuration access to the SIS during normal operation through a mechanism that requires the SIS to be unlocked to configure it, and locked at all other times. Having this capability means that the service provider is able to ensure that the SIS can be locked to prevent configuration changes from being made and unlocked to allow them to be made. Locks can be physical key switches or software controlled locks, but however implemented they allow the SIS to be locked to prevent inadvertent or malicious changes from being made.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.05.09	RE(1)	SIS	User interface	Configuration mode	No	The service provider shall have the capability to provide a hardware implementation of the configuration mode interface required by SP.05.09 BR and to ensure that ~~the Automation Solution provides a~~ this hardware implementation ~~of the interface required by SP.05.09 BR and that this hardware interface~~ is capable of being physically locked while configuration mode is disabled.	The capability specified by this RE is defined to require intentional human intervention to enable configuration of the SIS, such as holding a physical key open (unlocked) while the configuration is being changed, for the purpose of increasing confidence that inadvertent changes to the SIS configuration cannot occur. Having this capability means that the service provider is able to ensure that the SIS has a hardware interface that can be disabled to prevent configuration changes from being made. The hardware interface, such as a physical key switch, when physically locked (e.g. removing the key), configuration mode is disabled.
SP.05.09	RE(2)	SIS	User interface	Configuration mode	No	The service provider shall have the capability to have an independent 3rd party verify that it is not possible to change the configuration of the SIS when the hardware interface described in SP.05.09 RE(1) is locked in the "disable" configuration mode.	The capability specified by this RE is defined to add an additional level of confidence that the physical locking mechanism works as intended. Having this capability means that the service provider has an identifiable process for providing a report from a 3rd party that verifies that the SIS configuration locking mechanism works. This report may be initiated (e.g. contracted) by the control system supplier for the Automation Solution or by the service provider. This verification may occur prior to delivery of the product to the Automation Solution (as part of product verification) or after delivery of the hardware interface (as part of the service provider's its Automation Solution activities).

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.06.01	BR	Configuration management	Network design	Connectivity	No	The service provider shall have the capability to provide accurate logical and physical infrastructure drawings/documentation of the Automation Solution, including its network devices, internal interfaces, and external interfaces. The documentation and drawings shall be maintained as an accurate representation of the Automation Solution.	The capabilities specified by this BR and its RE are used to ensure that an accurate representation of the Automation Solution network architecture is documented and available for security-related activities, such as risk assessments and forensic analysis. Having this capability means that the service provider has an identifiable process for keeping its network architecture documentation current. The network architecture includes each network segment, the network devices used to interconnect the network segments, and an identification of all network interfaces internal to the Automation Solution and those that connect the Automation Solution to external networks. Network interfaces can be identified through a variety of techniques, including Ethernet addresses (i.e. MAC addresses), IP addresses, and network interface card identifiers. The intent is to provide enough information about them to unambiguously identify them. Risk assessments, zones (network segments), and conduits (connections between network segments), as described in IEC 62443-3-2, can be used in the development of the network architecture.
SP.06.01	RE(1)	Configuration management	Network design	Connectivity	No	The service provider shall have the capability to keep the as-built and installed equipment connection and configuration documents current.	Having this capability means that the service provider has an identifiable process for keeping its documentation up-to-date that describes the devices connected to each network segment in the Automation Solution. EXAMPLE For an Ethernet device, the documentation would include the network address and switch to which the device is connected, and a copy of the download file used to configure the device.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.06.02	BR	Configuration management	Devices – All	Inventory register	No	The service provider shall have the capability to create and maintain an inventory register, including version numbers and serial numbers, of all devices and their software components in the Automation Solution for which the service provider is responsible.	The capability specified by this BR is used to ensure that a component inventory is maintained to make it possible to determine if a component in the Automation Solution is authorized, and also to be able to determine if a vulnerability newly discovered within the industry is applicable to the Automation Solution. For example, if a vulnerability to a specific version/patch level is discovered, it should be possible to consult the Automation Solution inventory to determine if the vulnerability is applicable to devices/components used in the Automation Solution. Having this capability means that the service provider has an identifiable process for providing documentation for all components of the Automation Solution for which it is responsible. Characteristics include information such as model numbers, version numbers, and serial numbers. Documentation may include reports, automatically generated configuration data, screen captures, etc.
SP.06.03	BR	Configuration management	Devices – Control and instrumentation	Verification	No	The service provider shall have the capability to verify that wired and wireless devices used for control and instrumentation have been configured correctly with their approved values.	The capability specified by this BR is used to verify the integrity of device configurations. The intent is to be able to detect unauthorized or erroneous configuration changes. Having this capability means that the service provider has an identifiable process for verifying that device configuration parameters values have been correctly downloaded/written to the device. EXAMPLE Configuration parameter values can be confirmed by viewing them from a workstation.
SP.07.01	BR	Remote access	Security tools and software	Connectivity	No	The service provider shall have the capability to ensure that all remote access applications used in the Automation Solution are commonly accepted by both the security and industrial automation communities.	The capability specified by this BR is used to ensure that remote access applications provide acceptable levels of protection to the Automation Solution. Having this capability means that the service provider has an identifiable process for ensuring that all remote access applications are supported by commonly accepted remote access mechanisms (e.g. RDP). Remote access clients may be provided by the client and/or the service provider.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.07.02	BR	Remote access	Security tools and software	Technical description	No	The service provider shall have the capability to provide detailed instructions for the installation, configuration, operation, and termination of the remote access applications used in the Automation Solution.	The capability specified by this BR is used to ensure that remote access applications provide acceptable levels of protection to the Automation Solution. Having this capability means that the service provider has documentation for installing, configuring, and operating remote access applications that it recommends for use in the Automation Solution. The service provider is also required to provide instructions to the asset owner for the termination of these connections. The service provider is not permitted to establish remote access connections that cannot be terminated by the asset owner.
SP.07.03	BR	Remote access	Security tools and software	Technical description	No	The service provider shall have the capability to provide information about all proposed remote access connections to the asset owner that includes, for each connection: 1) its purpose, 2) the remote access application to be used, 3) how the connection will be established (e.g. via the Internet through a VPN), and 4) the location and identity of the remote client.	The capability specified by this BR is used to ensure that remote access to the Automation Solution is documented and managed to thwart unauthorized attempts to gain remote access to the Automation Solution. Having this capability means that the service provider has an identifiable process for defining and informing the asset owner of the details of all proposed remote access connections. The proposed location of the remote access client is required to be documented to allow the asset owner to review and approve/disapprove remote access from specific locations. In some cases, the proposed location may indicate “roaming” to allow for portable devices to be used as clients. It is not anticipated that the Automation Solution can automatically verify the physical location of the client at runtime.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.07.04	BR	Remote access	Security tools and software	Approval	No	The service provider shall have the capability ensure that it obtains approval from the asset owner prior to using each and every remote access connection.	The capability specified by this BR is used to ensure that all remote access connections to the Automation Solution are authorized by the asset owner. Having this capability means that the service provider has an identifiable process for using only those connections that have been approved by the asset owner. These remote access connections may be user-to-system or system-to-system, may traverse the Internet and/or include the use of modems, and/or may be provided and maintained by the asset owner. Requirements for management of these connections and the time needed by the asset owner to approve the connections are beyond the scope of this requirement. In addition, the asset owner may request the service provider to provide or maintain the connections and may provide the appropriate requirements at that time. For example, the asset owner may not allow TCP/IP protocols to be used over external connections that use modems. A risk assessment, as described in IEC 62443-3-2, may be used to define these requirements, including whether or not the connection should be encrypted, and whether or not a modem can be used to provide the connection, and if so, whether the modem should be disconnected when not in use, and whether the modem should be capable of being used as a router.
SP.07.04	RE(1)	Remote access	Data protection	Cryptography	No	The service provider shall have the capability to ensure that all remote access connections conducted over the Internet or over other publically accessible media that are used to support remote access to the Automation Solution by the service provider (e.g. from a service provider facility) are authenticated and encrypted.	The capability specified by this RE is defined to ensure that all connections used to support remote access to the Automation Solution by the service provider are protected. Service providers often offer remote support and troubleshooting/diagnostic services to the Automation Solution. Having this capability means that the service provider has an identifiable process for using encrypted links, such as VPNs, for remote access to the Automation Solution over the Internet by the service provider (e.g. from its facilities or other remote locations). Authentication is required to ensure that only authorized remote clients have access to the Automation Solution. In general, this requirement addresses the need for remote access to the Automation Solution by the service provider to support activities such as remote support.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.08.01	BR	Event management	Events – Security compromises	Responding	No	The service provider shall have capabilities for handling cyber-security incidents that affect the Automation Solution that include: 1) detecting cyber-security compromises and incidents, 2) reporting cyber-security incidents to the asset owner, 3) responding to cyber-security compromises and incidents, including supporting an incident response team. NOTE 1 Logging of security-related events is addressed by SP.08.02 BR. NOTE 2 Logging and reporting of alarms and events is addressed by SP.08.03 BR.	The capabilities specified by this BR and its REs are used to ensure that security incidents relevant to the Automation Solution are managed from detection through disposition to allow the security risk position of the Automation Solution to be maintained. Having this capability means that the service provider has an identifiable process for detecting, handling and reporting cyber-security incidents for Automation Solution components for which the service provider is responsible. What constitutes an incident, which incidents are significant, and under what conditions they are reported to the asset owner are all part of the service provider's incident handling procedures. Incident handling implementation may be controlled by specific agreements between the asset owner and service provider, such as non-disclosure agreements and/or other contractual vehicles between the asset owner and service provider. These contractual vehicles often identify proprietary data to be protected and the types of compromise that to be reported. Typically, the process of identifying incidents includes (1) event analysis and correlation, and (2) examination and triage of resulting compromises and potential incidents to yield incidents. SP.03.03 BR addresses handling of vulnerabilities that may have been exposed by this process or by other processes. In many cases, recognition that a compromise has occurred and that an associated loss has resulted can be difficult and may involve subjectivity and judgment. The specification of this process and the precise definition of what constitutes an incident is beyond the scope of these requirements. For requirements related to product development incident reporting and handling that can complement the service provider’s incident handling capabilities, see IEC 62443-4-1 and ISO/IEC 30111.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.08.01	RE(1)	Event management	Events – Security compromises	Reporting	No	The service provider shall have the capability to ensure that security compromises that have been automatically detected can be reported through a communications interface that is accessible to the asset owner and that is commonly accepted by both the security and industrial automation communities.	Having this capability means that the service provider has an identifiable process for reporting security compromises in security that it detects automatically. Security compromises are to be reported whether or not they result in a loss or are classified as an incident. Security compromises can be automatically detected at the time of compromise or through subsequent event analysis and correlation activities (e.g. through the use of a Security Information and Event Management (SIEM) package).
SP.08.02	BR	Event management	Events – Security-related	Logging	No	The service provider shall have the capability to ensure that the Automation Solution is configured to write all security-related events, including user activities and account management activities, to an audit log that is kept for the number of days specified by the asset owner. NOTE Logging and reporting of process-related events, such as setpoint changes and other operational/configuration data changes, is addressed by SP.08.03 BR.	The capabilities specified by this BR and its REs are used to ensure that security-related audit logs are supported. Audit logs can be used in forensics (e.g. who changed a user account and when) and in event correlation activities that may lead to security incident identification. Audit logs require a higher level of integrity protection than provided by typical event logs. They are used to protect against claims that repudiate responsibility for an action. Having this capability means that the service provider has an identifiable process to provide audit logging for security-related events that include successful and invalid logins and logouts, and creation, modification or deletion of user accounts, among others.
SP.08.02	RE(1)	Event management	Events – Security-related	Reporting	No	The service provider shall have the capability to ensure that security-related data and events can be accessed through one or more interfaces that is/are commonly accepted by both the security and industrial automation communities.	Having this capability means that the service provider has an identifiable process for ensuring that it is possible for the asset owner to collect security data and events over the network. Commonly accepted interfaces include interfaces that support polling (SNMP reads), asynchronous reporting (e.g. SNMP traps), and logging (e.g. Syslog, Syslog-ng and Common Event Format (CEF)). Use of commonly accepted interfaces make it easier to integrate off-the-shelf software packages that collect and analyze data and events. EXAMPLE Network devices typically maintain an SNMP Management Information Base (MIB) that contains security-related data that can be accessed using SNMP.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.08.02	RE(2)	Event management	Events – Security-related	Logging	No	The service provider shall have the capability to verify that, using a simulated security-related event approved by the asset owner, security-related events can be written to an audit log.	Having this capability means that the service provider has an identifiable process for verifying that the mechanisms used to log and report security-related events operate as required by SP 08.02 BR and SP 08.02 RE(1). Audit logs require a higher level of integrity protection than provided by typical event logs. They are used to protect against claims that repudiate responsibility for an action.
SP.08.03	BR	Event management	Events – Alarms & Events	Logging	No	The service provider shall have the capability to ensure that the Automation Solution is configured to log and notify the operator of process-related events as required by the asset owner. The types of events include state changes/operating condition changes/configuration changes that may be due to manual or automated (those without human intervention) operation. NOTE 1 Logging of security-related events is addressed by SP.08.02 BR.	The capabilities specified by this BR and its RE are used to ensure that process-related event logs are supported. Event logs can be used in forensics (e.g. who changed a setpoint and when) and in event correlation activities that may lead to security incident identification. Having this capability means that the service provider has an identifiable process for ensuring that the Automation Solution supports logging and notification of process-related events, and for configuring it to log and notify operators of events designated by the asset owner. Notifications include both simple event notifications and alarm/alert notifications. Alarms and events to be logged and reported include both operating system events and control system alarms and events. Events reported through this interface may be determined to require safeguarding as required by risk assessment, (see SP.03.01 BR and its REs). See also SP.03.10 BR and its REs for requirements for the protection of sensitive data. NOTE 2 Alarms and alerts, as defined by ISA 18.2 or NAMUR NA102, are notifications that require operator response (alarm) or awareness (alert).
SP.08.03	RE(1)	Event management	Events – Alarms & Events	Reporting	No	The service provider shall have the capability to ensure that alarms/alerts/events can be securely reported through an interface that is commonly accepted by both the security and industrial automation communities.	Having this capability means that the service provider has an identifiable process for ensuring that the Automation Solution is able to report alarms and events to external applications, such as a centralized log, through a commonly accepted interface that protects the transmitted events against tampering and disclosure. This interface may support event notifications or event polling.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.08.04	BR	Event management	Events – Alarms & Events	Robustness	~~No~~ Yes	The service provider shall have the capability to ~~ensure that the Automation Solution is able~~ document the Automation Solution's ability to withstand the near-simultaneous occurrence of large numbers of events, typically referred to as event storms.	The capability specified by this BR is used to ~~ensure that the Automation Solution does not suffer~~ document the limits of the Automation Solution's ability to protect against denial of service during event storms. The characteristics of event storms (e.g. number of events/second) ~~is~~ are typically dependent on the number of control and instrumentation devices in the Automation Solution and the nature of the physical process. Having this capability means that the service provider has an identifiable process for ~~ensuring that it is able to configure the Automation Solution with components that protect it against event storms~~ providing documentation that describes the limits of the Automation Solution's ability to handle event storms. Robustness testing and stress testing ~~is~~ are often used to demonstrate this assurance.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.09.01	BR	Account management	Accounts – User and service accounts	Administration	No	The service provider shall have the capability to ensure that the Automation Solution supports: 1) the use of a single, integrated data base, which may be distributed or redundant, for defining and managing user and service accounts, , 2) restricted management of accounts to authorized users, 3) decentralized access to this data base for the management of accounts, 4) decentralized enforcement of the account settings (e.g. passwords, operating system privileges, and access control lists) defined in this data base.	The capability specified by this BR is used to simplify the management of user accounts for Automation Solutions composed of multiple workstations and servers. Without such capabilities, separately managing accounts across individual workstations and servers often results in inconsistencies that result in denial of service to resources and/or the inappropriate granting of access to resources. Having this capability means that the service provider is able to ensure that the Automation Solution provides an account management system that: 1) has a single data base that may be distributed or redundant, as determined by Automation Solution requirements, 2) allows accounts, including user, administrator/super user accounts, and service accounts (i.e. accounts that do not provide for interactive login), to be defined and managed only by authorized users, 3) allows administrators to manage accounts from a specified set of workstations/servers in the Automation Solution, not just from a single dedicated workstation, 4) distributes the enforcement of account access control lists and privileges to the location where the access or privilege is to be executed. Examples of this type of account management include Lightweight Directory Access Protocol (LDAP) based technologies such as Windows Active Directory. See IEC 62443-3-3 for related security requirements for systems used in Automation Solutions.
SP.09.02	BR	Account management	Accounts – User and service accounts	Administration	No	The service provider shall have the capability to ensure that unique accounts can be created and maintained for users.	The capability specified by this BR is used to prevent users from having to share accounts, i.e. by having a separate account. Having this capability means that the service provider has an identifiable process for creating and maintaining a unique user account for each Automation Solution user.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.09.02	RE(1)	Account management	Accounts – User and service accounts	Technical description	Yes	The service provider shall provide documentation to the asset owner that: 1) identifies all default user and service accounts, 2) describes the tools and procedures used to set/reset passwords for all default user and service accounts.	The capability specified by this RE is defined to ensure there are no hidden accounts nor are there passwords that cannot be changed. Having this capability means that the service provider has an identifiable process for generating a list of all user and service accounts and providing instructions to the asset owner that describes how to change their passwords. For accounts used by services and servers (e.g. DCOM server), changing a password may involve one or more of the following: 1) changing the password for the account, 2) changing the "logon" password in the services/services that run under the account, 3) changing the password used by other software processes that connect to other processes using the account.
SP.09.02	RE(2)	Account management	Accounts – User and service accounts	Administration	No	The service provider shall have the capability to ensure that if an account/password is automatically generated for a user, other than operators and service groups, both the generated account and password are unique.	The capability specified by this RE is defined to ensure that the same password is not generated for multiple user accounts, other than for operator and service groups. Having this capability means that the service provider has an identifiable process for verifying that the Automation Solution does not generate the same password for two different users and that each generated user account is unique and has a unique identifier. This requirement does not apply to Automation Solutions that do not generate accounts and passwords for individual users.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.09.02	RE(3)	Account management	Accounts – User and service accounts	Expiration	No	The service provider shall have the capability to ensure that service, auto-login and operator accounts, and other accounts required for essential functions and/or continuous operations, or as required by the asset owner have been configured so that they never expire nor become disabled automatically.	The capability specified by this RE is defined to prevent services, operators, workstations configured for auto-login, and other accounts as required, from experiencing denial of service because their accounts have expired or become automatically disabled. Having this capability means that the service provider has an identifiable process for ensuring that accounts that are permanent accounts in the Automation Solution, such as service, auto-login and operator accounts, are configured so that they do not expire or become automatically disabled or deleted. Operator accounts are typically individual user accounts configured with operator privileges that provide visibility into the physical environment (e.g. the process) being controlled. This requirement does not prevent permanent accounts from being removed, or otherwise disabled, based on explicit actions taken by an administrator. A commonly recommended measure for Unix-based systems is to configure the root account to use the false or “nologin” shell (and thus effectively denying all logins using this account) and creating a differently named alias for the root account for use by authorized administrative users. NOTE See SP.03.01 BR and its REs for assessing and addressing risks associated with accounts that do not expire.
SP.09.02	RE(4)	Account management	Accounts – Administrator	Least functionality	No	The service provider shall have the capability to ensure that the built-in administrator account is disabled, and if that is not possible, that it is renamed or otherwise made difficult to exploit.	The capability specified by this RE is defined to make it difficult for attackers to gain administrative privileges using the built-in administrator account. Having this capability means that the service provider has an identifiable process for disabling or renaming the built-in administrator account, or if neither of those is possible, making it difficult to recognize and exploit it. Providing access to the built-in administrator account allows malware to potentially use this account and gain control of the system. NOTE Renaming is not as effective since the operating system may not change the underlying identifier for the account.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.09.03	BR	Account management	Accounts – Default	Least functionality	No	The service provider shall have the capability to ensure that unused system default accounts have been removed or disabled.	The capability specified by this BR is used to prevent attackers from gaining access to the Automation Solution through unused system default accounts. Having this capability means that the service provider has an identifiable process for removing system default (built-in) accounts that are not needed for the Automation Solution. Built-in accounts are generally installed when new computers (e.g. workstations) are added to the Automation Solution or when their software is installed or reinstalled. This requirement applies to all default system accounts, whether they are installed with the operating system or with control system or related software. The service provider needs to have a process for ensuring unnecessary built-in accounts are removed.
SP.09.04	BR	Account management	Accounts – User	Least functionality	No	The service provider shall have the capability to ensure that all user accounts are removed once they are no longer needed. This includes: 1) temporary accounts under the control of the service provider, such as those used for integration or maintenance, 2) user accounts for service provider personnel who are no longer assigned to the Automation Solution (see SP.01.07 BR for notifying the asset owner of the removal of service provider personnel from the Automation Solution.	The capabilities specified by this BR and its RE are used to prevent attackers from gaining access to the Automation Solution through accounts that are not needed (e.g. accounts of users who are no longer assigned to the Automation Solution). Having this capability means that the service provider has an identifiable process for removing or disabling accounts that were created to support its personnel once their activities are complete or their assignment to the Automation Solution has ended. The intent is to ensure that the Automation Solution does not contain or retain service provider accounts unless they are needed.
SP.09.04	RE(1)	Account management	Accounts – User	Logging	No	The service provider shall have the capability to generate an audit log report after the completion of integration/maintenance activities that shows that accounts used to support these activities have been removed from the Automation Solution if they are no longer needed.	Having this capability means that the service provider has an identifiable process for producing a report that confirms that accounts that were created to support its activities have been removed once those activities are complete. The intent is to ensure that the Automation Solution does not contain or retain service provider accounts unless they are needed. See SP.08.02 BR for the requirement to log security-related events, which includes the removal of these accounts.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.09.05	BR	Account management	Passwords	Composition	No	The service provider shall have the capability to ensure that password policies can be set to achieve a minimum complexity commonly accepted by both the security and industrial automation communities. NOTE At the time of this writing, minimal password complexity is: 1) at least eight characters in length and 2) a combination of at least three of the following four character sets: lowercase, uppercase, numeric digit, and special characters (e.g.% and #).	The capability specified by this BR is used to ensure that the service provider can support a broad range of asset owner password complexity policies. Using complex passwords makes password discovery more difficult. Having this capability means that the service provider has an identifiable process for ensuring that the Automation Solution supports complex passwords. The password complexity used within a specific Automation Solution is beyond the scope of this requirement. See IEC 62443-3-3 for related security requirements for systems used in Automation Solutions, and IEC 62443-3-2 for the use of risk assessments to aid in the determination of the level of password complexity to be used for a specific Automation Solution. Also see IEC 62443-2-1 for password policy requirements for asset owners.
SP.09.06	BR	Account management	Passwords	Expiration	No	The service provider shall have the capability to ensure that passwords for local and system-wide (e.g. domain) user accounts are configured to automatically expire after they have been in use for a period of time specified by the asset owner.	The capabilities specified by this BR and its RE are used to ensure that passwords can be changed periodically. Passwords that remain unchanged increase the risk that they will be disclosed/discovered and used to gain unauthorized access to the system. In addition, changing passwords periodically limits the length of time an attacker has to discover a password. Having this capability means that the service provider has an identifiable process for ensuring that passwords can be configured to automatically expire after they have been in use for an asset owner specified number of days. When and how often the service provider verifies that the password expiration period is Automation Solution specific, but verification is typically done as part of the handover process and at after or during each maintenance cycle. The asset owner's security policy should set the expiration period based on a risk assessment and this value should be periodically be reviewed. See IEC 62443-3-2 for more information on risk assessment, IEC 62443-3-3 for related requirements for control systems product capabilities, and IEC 62443-2-1 for related requirements for asset owners. NOTE IEC 62443-2-1 does not explicitly mention lifetime requirements for passwords, but does address more general password policies.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.09.06	RE(1)	Account management	Passwords	Expiration	No	The service provider shall have the capability to ensure that password policies are set to prompt users to change passwords *N* days before they expire, where *N* is specified by the asset owner. This requirement does not apply to passwords that are not set to expire.	Having this capability means that the service provider has an identifiable process for ensuring that users are notified that their passwords are expiring so they have time to change them.
SP.09.07	BR	Account management	Passwords	Change	No	The service provider shall have the capability to ensure that default passwords are changed as required by the asset owner.	The capability specified by this BR is defined to prevent default passwords that have become well-known from being used in any Automation Solution. Having this capability means that the service provider has an identifiable process for ensuring that default passwords are changed according to asset owner requirements. Typically, this will be on installation, re-installation, and reset/recovery.
SP.09.08	BR	Account management	Passwords	Reuse	No	The service provider shall have the capability to ensure that password policies are set to prevent users from reusing their last *N* passwords, where *N* is specified by the asset owner.	The capabilities specified by this BR and the its RE are defined to prevent users from changing their passwords and then immediately changing them back, which would effectively mean that their passwords were not changed. Having this capability means that the service provider has an identifiable process for verifying that the password reuse policy is set to the number specified by the asset owner.
SP.09.08	RE(1)	Account management	Passwords	Change	No	The service provider shall have the capability to ensure that password policies are set to prevent users from changing their passwords more frequently than once every N days, where N is specified by the asset owner.	Having this capability means that the service provider has an identifiable process for configuring password policies to prevent users from changing password continuously to get back to a favorite password. The period of *N* days means that once a password has been changed, the user cannot change it again for *N* days.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.09.09	BR	Account management	Passwords	Shared	No	The service provider shall have the capability to ensure that accounts whose passwords have been approved by the asset owner to be shared with the service provider are securely documented and maintained.	The capabilities specified by this BR and its RE are used to ensure that the use of shared passwords is managed. Without management of shared passwords, the asset owner may not be aware of or lose track of who has access to the Automation Solution. Having this capability means that the service provider has an identifiable process for ~~managing and protecting~~ documenting the list of accounts for which passwords have been divulged to it by the asset owner and protecting that list from unauthorized disclosure and modification. The service provider is accountable and responsible for maintaining a log of ~~the usage of each account by its personnel~~ who has been given passwords for these accounts, including its subcontractors, consultants, and representatives.
SP.09.09	RE(1)	Account management	Passwords	Shared	No	The service provider shall have the capability to report to the asset owner passwords that were 1) shared and no longer need to be shared, 2) knowingly divulged, or 3) knowingly compromised, and to support the asset owner in changing passwords as necessary.	Having this capability means that the service provider has an identifiable process for keeping track of passwords (including passwords for auto-login accounts) that were shared with the service provider or that the service provider knows were compromised or otherwise divulged to others, and for reporting them to the asset owner so they can be changed. For example, the service provider will need to report passwords shared within the service provider organization to the asset owner once they are no longer needed by the service provider. To change these passwords, the asset owner may require the service provider's support. Similarly, if service provider personnel share passwords with others, the service provider will need to report these accounts/passwords to the asset owner when they no longer need to be shared. Sharing of passwords often occurs during testing, commissioning, troubleshooting, and maintenance. In addition, any time the service provider suspects that a password has been compromised, it should notify the account owner and request that the password be changed.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.10.01	BR	Malware protection	Manual process	Malware protection mechanism	No	The service provider shall have the capability to provide the asset owner with documented instructions for the proper installation, configuration and update of malware protection mechanisms that are tested and verified for the Automation Solution.	The capability specified by this BR is used to ensure that the asset owner has the documentation necessary to use the anti-malware mechanisms that are compatible with the Automation Solution. Having this capability means that the service provider has an identifiable process for providing the documentation for commonly accepted malware protection software (e.g. anti-virus, whitelisting) that operates as intended on Automation Solution hardware platforms (e.g. workstations) for which the service provider is responsible. If the control system supplier does not test and recommend an anti-malware product, then the service provider needs to be able to have these capabilities.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.10.02	BR	Malware protection	Security tools and software	Installation	No	The service provider shall have the capability to ensure that: 1) malware protection mechanisms have been correctly installed/updated and properly configured in accordance with the service provider's approved procedures, 2) malware definition files are installed within the time period agreed to with the asset owner, 3) malware configurations are maintained and kept current.	The capabilities specified by this BR and its RE are used to ensure that the Automation Solution is protected against malware. Having this capability means that the service provider has an identifiable process for ~~installing, updating, and configuring~~ applying and managing anti-malware software for Automation Solution platforms for which the service provider is responsible. This includes installing and updating anti-malware software, keeping its malware definition files current, and maintaining its operational configuration settings. The intent is to have anti-malware software with its latest ~~data~~ definition files, operational configuration, and software updates running on all relevant hardware platforms in the Automation Solution. Having this capability also means that the service provider has an identifiable process for coming to agreement with the asset owner on the time period between the release of the malware definition files and their installation. EXAMPLE 1 If anti-virus software is used, installation of anti-virus definition files is performed within the agreed-to time period. EXAMPLE 2 If whitelisting software is used, whitelisting configurations are kept current. EXAMPLE 3: Keeping a log of the installation and configuration activities, including updates to software and malware definition files, is a way of demonstrating this capability.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.10.02	RE(1)	Malware protection	Security tools and software	Installation	No	The service provider shall create and maintain the documentation that describes the use of malware protection mechanisms in the Automation Solution for which the service provider is responsible. This documentation shall include for each component used in the Automation Solution: 1) the installation state of malware protection mechanisms or a statement that it is not technically possible to install malware protection mechanisms on the component, 2) the current configuration settings of the installed malware protection mechanism, 3) the current status of malware definition files approved for installation on the component, 4) the use of other mitigating features and functions used to reduce the risk of infection and/or mitigate the effect of infections (e.g. isolating infections, reporting infections).	Having this capability means that the service provider has an identifiable process for documenting the anti-malware software status for each hardware platform in the Automation Solution, whether or not anti-malware software is installed on the component. All platforms are required to have anti-malware software installed, except where it is not technically feasible (e.g. no anti-malware software exists).
SP.10.03	BR	Malware protection	Security tools and software	Detection	No	The service provider shall have the capability to verify that malware, other than zero-day malware, can be detected and properly handled by the installed malware protection mechanisms.	The capability specified by this BR is used to verify that anti-malware mechanisms work as intended. Having this capability means that the service provider has an identifiable process for verifying that an infected file can be detected and subsequently quarantined/deleted by the anti-malware product. The only exception is a zero-day infection, which is an infraction for which there is no malware definition file available. This is generally the case when the malware has not been previously seen or detected.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.10.04	BR	Malware protection	Manual process	Malware definition files	Yes	The service provider shall have the capability to provide to the asset owner documentation that describes: 1) how malware definition files for the Automation Solution are evaluated and approved, 2) reporting the status of malware definition files to the asset owner within *N* days after release of the files by the manufacturer, where *N* has been agreed to by the service provider and asset owner. This status includes the applicability (e.g. component and version) and approval state (e.g. approved, installed, disapproved, etc.) for each malware definition file.	The capability specified by this BR is used to ensure that service provider has a process for verifying that new malware definition files are compatible with the Automation Solution and that they are available to the Automation Solution in a timely manner. Having this capability means that the service provider has an identifiable process for approving malware definition files and informing the asset owner of the results within a mutually agreed to time period after their release by the anti-malware software manufacturer. This does not require installation within this time-period, it requires only that files are approved for installation within the time period. Approval means that the service provider has evaluated the files for conflicts with their system. Those that conflict with the operation of the system are not approved.
SP.10.05	BR	Malware protection	Devices – All	Sanitizing	No	The service provider shall have the capability to ensure that all devices, including workstations, supplied to the Automation Solution by the service provider are free of known malware prior to use in the Automation Solution.	The capability specified by this BR is used to ensure that devices with detectable infections are not installed in the Automation Solution. The term “known malware” is used to indicate malware that has been previously discovered and for which malware definition files have been developed and are available. Having this capability means that the service provider has an identifiable process for verifying/ensuring that malware is not present in equipment provided by it to the Automation Solution. Verification can include checking the equipment for malware, installing software to the equipment at the site from malware-free media (see SP.10.05 RE(2)), and/or ensuring the supply chain provides malware free equipment (e.g. the control system vendor performs malware scans prior to delivery). See ISO 27036 for more information on supply chain security.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.10.05	RE(1)	Malware protection	Portable media	Usage	No	The service provider shall have the capability to ensure that for portable media that it uses for system testing, commissioning, and/or maintenance, it uses this portable media for this purpose only.	The capability specified by this RE is used to ensure that portable media are not used outside the Automation Solution to reduce the possibility of them becoming infected with malware. Having this capability means that the service provider has an identifiable process for ensuring that it does not use portable media that it uses in support of the Automation Solution (that has the possibility of infecting the Automation Solution with malware) in other places where it could be infected. For example, if a USB memory device has diagnostics tools or data on it, then this device should not be connected to any workstation or server that is not part of the Automation Solution.
SP.10.05	RE(2)	Malware protection	Portable media	Sanitizing	No	The service provider shall have the capability to ensure that all portable media~~, including installation media and portable computers,~~ used in or connected to the Automation Solution by the service provider is free of known malware prior to use in the Automation Solution.	The capability specified by this RE is used to ensure that portable media with detectable infections are not used in the Automation Solution. The term “known malware” is used to indicate malware that has been previously discovered and for which malware definition files have been developed and are available. Having this capability means that the service provider has an identifiable process for~~ has~~ procedures to prevent infected portable devices from infecting the Automation Solution. Types of portable media include but are not limited to: installation media, CD / DVD/ Blu-ray Media, USB memory devices, smart phones, flash memory, solid state disks, hard drives, and portable computers. See SP.07.XX for requirements associated with remote connection to the Automation Solution.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.11.01	BR	Patch management	Manual process	Patch qualification	Yes	The service provider shall have the capability to provide documentation to the asset owner that describes how security patches for Automation Solution software for which it is responsible are evaluated and approved. NOTE 1 In this standard, firmware upgrades are regarded as software patches. NOTE 2 In this standard, patch installation refers to installation of patches to the Automation Solution.	The capability specified by this BR is used to ensure that service provider has a documented process that can be reviewed by the asset owner for verifying that new software security patches are compatible with the Automation Solution (see SP.10.04 BR). In many cases, the service provider will use documentation from the control system product supplier and modify it for the Automation Solution if necessary. Having this capability means that the service provider has an identifiable process for providing a document to the asset owner that describes its policies for determining which security patches apply to the Automation Solution, and how they are tested and approved. This includes security patches for the control system and component software, operating system software, and 3rd party software applications integrated into or with the Automation Solution, the control system, and components. IEC TR 62443-2-3 describes patch management and outlines a set of associated responsibilities for the control system supplier and the asset owner. SP 11.XX defines patch management capabilities for the service provider in support of the IEC TR 62443-2-3 asset owner patch management responsibilities.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.11.01	RE(1)	Patch management	Manual process	Patch qualification	No	The service provider shall have the capability to review, as a result of changes in security risks, how it evaluates and approves security patches for Automation Solution software for which it is responsible.	The capability specified by this RE is used to ensure that service provider is able to update its patch evaluation process in response to changes in the cyber-security threat landscape. (e.g. new threats may require a more rapid response). Typically, this is demonstrated as part of its incident handling capabilities or as a separate process for periodically reviewing its patch evaluation process. Having this capability means that the service provider has an identifiable process for reviewing its process for evaluating and approving security patches. These reviews are required to be performed to be able to update this process to address changes in the risk environment. This review needs to be performed periodically or explicitly in response to significant changes in the risk environment. Significant changes are those that are recognized to have a potential impact on the process. Changes to the risk environment generally includes new threats and vulnerabilities as well as the development of new security technologies.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.11.02	BR	Patch management	Patch list	Patch qualification	Yes	The service provider shall have the capability to make documentation available to the asset owner that describes security patches/updates. The description of each patch shall be available to the asset owner within an agreed time frame after the release of a patch by its manufacturer, and shall include: 1) security patches that are applicable to components of the Automation Solution for which the service provider is responsible, 2) the approval status/lifecycle state (see IEC TR 62443-2-3) of each; i.e., approved, not approved, not applicable, in test, 3) a warning if the application of an approved patch requires or causes a re-start of the system, 4) the reason for those that are not approved or not applicable, 5) a plan for the remediation for those that are applicable but not approved.	The capabilities specified by this BR and its REs are used by the asset owner to access descriptions of security patches that are relevant to the Automation Solution from the service provider and to have the service provider recommend how to mitigate vulnerabilities for patches the asset owner choose not to install. Having this capability means that the service provider has an identifiable process for evaluating and approving security patches as documented by the capability defined in SP.11.01 BR, and for informing the asset owner of the results within *N* number of days after the release of the patch by its manufacturer, where *N* is agreed to by the service provider and the asset owner. The service provider may use software libraries that are enhanced or otherwise different than those provided by their manufacturer(s). In this case, the service provider may need to alter a software patch package. This type of issue needs to be addressed as part of this requirement.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.11.02	RE(1)	Patch management	Patch list	Patch qualification	No	The service provider shall have the capability to make available to the asset owner, through an interface commonly accepted by the industrial and security communities, a patch list that identifies: 1) approved security patches applicable to Automation Solution software for which the service provider is responsible (e.g. control system and component software, operating system software, and 3rd party software applications), 2) which of the applicable security patches have been approved for use in the Automation Solution, 3) the version numbers of the software to which the approved patches apply. This list shall be available to the asset owner within an agreed timeframe after the release of a patch by the manufacturer.	Having this capability means that the service provider has an identifiable process for describing to the asset owner how to electronically retrieve a list that describes the approved security patches that are applicable to components for which the service provider is responsible (see SP.11.02 BR). This list is to be provided through a commonly accepted interface to allow the asset owner to know which patches it needs to download from the manufacturer or obtain otherwise obtain them. This list may be retrieved through this interface from the control system product supplier, from the service provider, or from another agent identified by the service provider. NOTE Approved is meant to imply that the patches have been tested and validated by the service provider against a known configuration and no issues were found.
SP.11.02	RE(2)	Patch management	Patch list	Approval	No	The service provider shall have the capability to: 1) recommend a mitigation plan when requested by the asset owner for security patches that were applicable and approved by the service provider, but that were not approved by the asset owner, for example, because they could impact operations or performance (see SP 11.05 BR), 2) implement the mitigation plan after approval by the asset owner.	Having this capability means that the service provider has an identifiable process for developing and implementing an approach to mitigate the impact of not being permitted to install a security patch that could negatively impact the Automation Solution. This approach may include compensating mechanisms or other means to reduce the vulnerabilities addressed by the security patch. Alternative approaches are subject to asset owner approval.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.11.03	BR	Patch management	Security patch	Delivery	No	The service provider's management of patches shall provide for: 1) patches to be obtained by the asset owner directly from the patch's manufacturer, and/or 2) redistribution of patches by the service provider only if approved by the asset owner and permitted by the patch manufacturer.	The capability specified by this BR is used to ensure that patches are obtained through an authorized channel (from an appropriate source) to reduce the possibility that they could be invalid/infected. Having this capability means that the service provider's patch delivery policy supports having the asset owner obtain the patch directly from the patch manufacturer, or from the service provider at the request of the asset owner, and then only if the licensing agreements with the patch manufacturer permit this. If the patches are to be delivered by the service provider, then the service provider and the asset owner will have to jointly decide how this will occur (e.g. DVD, secure connection).
SP.11.04	BR	Patch management	Security patch	Installation	Yes	The service provider shall have the capability to provide documentation to the asset owner that describes how to perform patching both manually and via a patch management server and how to obtain patching status reports. 1) When using a patch management server, documentation shall be provided to show how to use the server to install patches. 2) For manual patching using portable media, documentation shall be provided that describes how to install patches from the media.	The capability specified by this BR is used to ensure that the asset owner knows how to install security patches for the Automation Solution. Having this capability means that the service provider is able to provide instructions to the asset owner that describes how to install patches from portable media (e.g. CDs, DVDs, USB memory devices) and from a patch management server.
SP.11.05	BR	Patch management	Security patch	Approval	No	The service provider shall have the capability ensure that it obtains approval from the asset owner for installing each and every security patch.	The capability specified by this BR is used to ensure that the service provider installs patches if and only if the asset owner wants them to be installed. Having this capability means that the service provider has a policy that requires it to obtain approval from the asset owner to install patches.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.11.06	BR	Patch management	Security patch	Installation	No	The service provider shall have the capability to ensure that if the asset owner requests the service provider to install security software patches (including firmware upgrades), the service provider installs them at a time specified by the asset owner.	The capability specified by this BR is used to ensure that the service provider installs patches only when the asset owner wants them to be installed, for example, to prevent process upset if a device has to reboot after installation. Having this capability means that the service provider has an identifiable process for installing approved patches only at a time specified by the asset owner.
SP.11.06	RE(1)	Patch management	Security patch	Installation	No	The service provider shall have the capability to ensure that the security hardening level of the Automation Solution is retained after patch installation, e.g. by reinstalling software or changing system configuration settings.	The capability specified by this RE is used to ensure that patch installation does not "undo" or otherwise degrade the hardening of the Automation Solution. Having this capability means that the service provider has an identifiable process for ensuring that it has a process for restoring the hardening state of the Automation Solution if patch installation causes it to degrade. This capability is independent of who installs the patches. It is not uncommon for the installation of patches and system updates to require or automatically restore configuration settings that remove or degrade system hardening, such as the installation of a Service Pack from Microsoft. Therefore, the service provider has to have a process that determines if this has happened, and if it has to restore the hardening.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.11.06	RE(2)	Patch management	Security patch	Installation	No	The service provider shall have the capability to ensure that, for devices that support installation of software/firmware over the network, the update process ensures the authenticity and integrity of the device software/firmware.	The capability specified by this RE is used to ensure that patches installed over the network are authentic and have not been corrupted prior to or during the patching process. Having this capability means that the service provider has an identifiable process for securely updating the software/firmware in devices. This includes allowing only authorized users to perform updates, and also ~~that the update image sent to the device is protected during transmission against modification~~ ensuring that update images sent to devices are authentic (not counterfeit or corrupted) and are protected against corruption during the update process. Patching may expose software images to the network. See SP.03.10 BR and its REs for the safeguarding of sensitive data. See IEC 62443-3-3 and IEC 62443-4-2 for requirements related to authentication, authorization, integrity, and confidentiality.
SP.11.06	RE(3)	Patch management	Security patch	Installation	No	The service provider shall have the capability to determine the installation status of all security patches applicable to the Automation Solution for which the service provider is responsible.	Having this capability means that the service provider has an identifiable process for tracking whether patches approved for the Automation Solution have been installed for the purpose of determining which patches are missing (not installed). This capability may be provided with either manual procedures or automated tools.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.12.01	BR	Backup/Restore	Manual process	Technical description	Yes	The service provider shall have the capability to provide documentation for recommended backup procedures for the Automation Solution that includes, but is not limited to the following: 1) Instructions on how to make a full backup of the Automation Solution, and partial backups if applicable, using at least one of the following methods a) proprietary backup architecture on removable media, b) single system backup architecture on removable media, c) distributed back-up architecture in which each backup system backs up a subset of the service provider's Automation Solutions at the asset owner's site, or d) centralized back-up architecture using one backup system for all fo the service provider's Automation Solutions at the asset owner's site.	The capability specified by this BR ensures that the asset owner knows how to use the backup capabilities provided by the service provider for the Automation Solution. Having this capability means that the service provider has an identifiable process for preparing a document specific to the Automation Solution that defines how to backup the Automation Solution, which data to backup to support full and partial backups, and how it recommends off-site storage to be handled. This documentation should recognize that: 1) The backup image is regarded as sensitive (see SP.03.10 BR and its REs for the safeguarding of sensitive data) and may therefore be a target for security compromise. 2) The backup may be needed to recover from security incidents (e.g. a workstation becomes corrupted). 3) The asset owner may have a backup strategy that is generally dependent of business requirements. 4) The asset owner's backup strategy may include topics related to backup frequency, partial backups, when backups should be performed (e.g. prior to engineering changes), and recovery from infection that may influence the contents of the service provider documentation. 5) Backups should be allowed to complete before changes are made that could interrupt the backup or that could cause inconsistencies in the backup data. Examples of such changes include engineering changes and patch installation.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
						2) Provisions to back-up the following types of data a) operation system files and cryptographic data (e.g. keying material), b) applications(including middleware, such as tunneling software), c) configuration data, database files, d) log files, electronic log book, e) unconventional file types including, but not limited to network equipment settings, control system controller settings (tuning parameters, set points, alarm levels), f) field instrumentation parameters, and g) directory information h) other files identified by the service provider that are required to create a complete backup of the Automation Solution, 3) Recommendations for offsite storage of backup media, 4) Provisions to ensure changes to the Automation Solution that could affect the integrity of a backup are not made while a backup is in progress NOTE Examples of partial restores include operating system, application software, databases, and configuration files.	

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.12.02	BR	Backup/Restore	Restore	Technical description	Yes	The service provider shall have the capability to provide documented instructions to the asset owner for restoring the Automation Solution or its components to normal operation.	The capability specified by this BR ensures that the asset owner knows how to use the restore capabilities provided by the service provider for the Automation Solution. Having this capability means that the service provider has an identifiable process for preparing or providing documentation that describes how to restore the Automation Solution or its components (i.e. a partial restore) from backup data. The documentation should include instructions for handling abnormal scenarios, such as how to restore an Automation Solution whose architecture may have changed since the backup was made. In these cases, the restore may not be complete and the asset owner should be made aware of conditions such as these. This requirement applies to both operational Automation Solutions and simulations.
SP.12.03	BR	Backup/Restore	Portable media	Technical description	Yes	The service provider shall have the capability to provide documentation to the asset owner that describes how to control and securely manage removable backup media.	The capability specified by this BR ensures that the asset owner knows how to securely handle the backup media for the Automation Solution. Having this capability means that the service provider has an identifiable process for preparing a document specific to the Automation Solution that describes handling of backup data to adequately protect it that is consistent with, or extensions of, asset owner policies and procedures. Backup data can be a target for compromise, for example, to prevent proper restoration or to gain access to confidential data.
SP.12.04	BR	Backup/Restore	Backup	Verification	Yes	The service provider shall have the capability to provide documentation to the asset owner that describes how to verify successful system backup.	The capability specified by this BR ensures that the asset owner knows how to verify the backup of the Automation Solution. Having this capability means that the service provider has an identifiable process for preparing (or providing) a document that describes how to verify the success of a backup.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.12.05	BR	Backup/Restore	Restore	Verification	No	The service provider shall have the capability to verify that: 1) it is possible to perform a complete back-up of the Automation Solution, and 2) it is possible to restore a fully functioning Automation Solution from this back-up.	The capability specified by this BR ensures that the backup and restore capabilities for the Automation Solution work as intended. Having this capability means that the service provider has an identifiable process for demonstrating or otherwise verifying that a backup can be performed successfully and that the Automation Solution can be restored from this backup. This process should be flexible to allow the asset owner to request only a partial backup/restore to gain confidence that the backup capability can be used successfully. If the backup includes the backup of data bases, then having this capability also means that the service provider has an identifiable process for demonstrating or otherwise verifying that automatic rollback is stopped/disabled prior to starting the backup. Automatic rollback can cause inconsistencies in the data base should it occur while the data base is being backed up.
SP.12.06	BR	Backup/Restore	Backup	Perform	No	The service provider shall have the capability to perform a backup of the Automation Solution in accordance with the asset owner's backup schedules and data restore and disaster recovery objectives.	The capability specified by this BR ensures that, when backing up the Automation Solution, the service provider follows the guidance/policies of the asset owner. Having this capability means that the service provider has an identifiable process for adhering to the asset owner's backup/restore strategies and objectives, including backup schedules and disaster recovery plans (see SP.12.09 BR). The intent of this requirement is to ensure that the service provider is prepared to integrate its backup/restore activities with the asset owner's backup requirements.
SP.12.07	BR	Backup/Restore	Backup	Robustness	No	The service provider shall have the capability to ensure that the Automation Solution is able to continue normal operation during a backup.	The capability specified by this BR ensures that operation of the Automation Solution (e.g. control of the process) is not impacted by the backup process. Having this capability means that the service provider has an identifiable process for ensuring that the backup operations do not interfere with normal operations of the Automation Solution. For related system capability requirements, see IEC 62443-3-3.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.12.08	BR	Backup/Restore	Manual process	Logging	Yes	The service provider shall have the capability to provide documentation to the asset owner that describes how to generate and maintain audit logs of all backup and restore activities.	The capability specified by this BR ensures that the asset owner knows how to manage audit logs for the backup and restore operations. These audit logs provide evidence of backup/restore activities such as when they occurred, who performed them, and their status. Having this capability means that the service provider has an identifiable process for preparing or providing documentation that describes how to configure the Automation Solution to write backup and restore actions to an audit log.
SP.12.09	BR	Backup/Restore	Manual process	Disaster recovery	Yes	The service provider shall have the capability to document a recommended disaster recovery plan that includes, but is not limited to the following: 1) Description of various disaster scenarios and their impact on the Automation Solution, 2) Step-by-step instructions for restoring, restarting, failed components and integrating them into the Automation Solution, 3) Minimum architecture requirement for restoring the entire Automation Solution.	The capability specified by this BR ensures that not only is there is a plan for recovering from a disaster, but also that the details of how a disaster could occur (e.g. including cyber-security threats), and how to recover from the disaster. Having this capability means that the service provider has an identifiable process for preparing a document specific to the Automation Solution that defines how to manage a major crisis based on a cyber-security scenario for restoring the Automation Solution and its components. The back-up and the means of restoration cannot be compromised by loss of the Automation Solution components or the entire Automation Solution. The means of restoration may include equipment, such as test bench or off-line development tools.

Bibliography

NOTE This bibliography includes references to sources used in the creation of this standard as well as references to sources that may aid the reader in developing a greater understanding of cybersecurity as a whole and of the process of developing a cybersecurity management system. Not all references in this bibliography are referred to throughout the text of this standard.

IETF/RFC 1510, The Kerberos Network Authentication Service (V5)

CMMI® for Services, Version 1.3, November 2010, (CMU/SEI-2010-TR-034, ESC-TR-2010-034)

ISO/IEC 27036-3, *Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security*

ISO/IEC 30111, *Information technology – Security techniques – Vulnerability handling processes*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*

IEC 62264-1:2013: *Enterprise-control system integration – Part 1: Models and terminology*

IEC 62351-8:2011, *Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control*

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

IEC/TR 62443-1-2, *Industrial communication networks – Network and system security – Part 1-2: Master glossary of terms and abbreviations*[1]

IEC/TR 62443-1-3, *Industrial communication networks – Network and system security – Part 1-3: System security compliance metrics*[2]

IEC 62443-2-1:2010 *Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program*

IEC/TR 62443-2-3, *Industrial communication networks – Network and system security Part 2-3: Patch management in the IACS environment*[3]

IEC 62443-3-2, *Industrial communication networks – Network and system security – Part 3-2: Security assurance levels for zones and conduits*[4]

[1] Under consideration.

[2] Under preparation.

[3] Under preparation.

IEC 62443-3-3:2013, *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*

IEC 62443-4-1, *Industrial communication networks – Network and system security – Part 4-1: Product development requirements*[5]

IEC 62443-4-2, *Industrial communication networks – Network and system security – Part 4-2: Technical security requirements for IACS components*[6]

IEC TR 62443-4-2-1, *Industrial communication networks – Network and system security – Part 4-2-1: WIB Profiles*[7]

____

[4] Under preparation.

[5] Under consideration.

[6] Under consideration.

[7] Under consideration.

IEC 62443-2-4

Edition 1.1 2017-08

FINAL VERSION

colour
inside

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

IEC 62443-2-4:2015-06+AMD1:2017-08 CSV(en)

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

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

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

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

DISCLAIMER
This Consolidated version is not an official IEC Standard and has been prepared for user convenience. Only the current versions of the standard and its amendment(s) are to be considered the official documents.

This Consolidated version of IEC 62443-2-4 bears the edition number 1.1. It consists of the first edition (2015-06) [documents 65/545/CDV and 65/561A/RVC] and its corrigendum 1 (2015-08), and its amendment 1 (2017-08) [documents 65/637A/CDV and 65/661/RVC]. The technical content is identical to the base edition and its amendment.

This Final version does not show where the technical content is modified by amendment 1. A separate Redline version with all changes highlighted is available in this publication.

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.

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 the base publication and its amendment 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.

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

INTRODUCTION

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

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

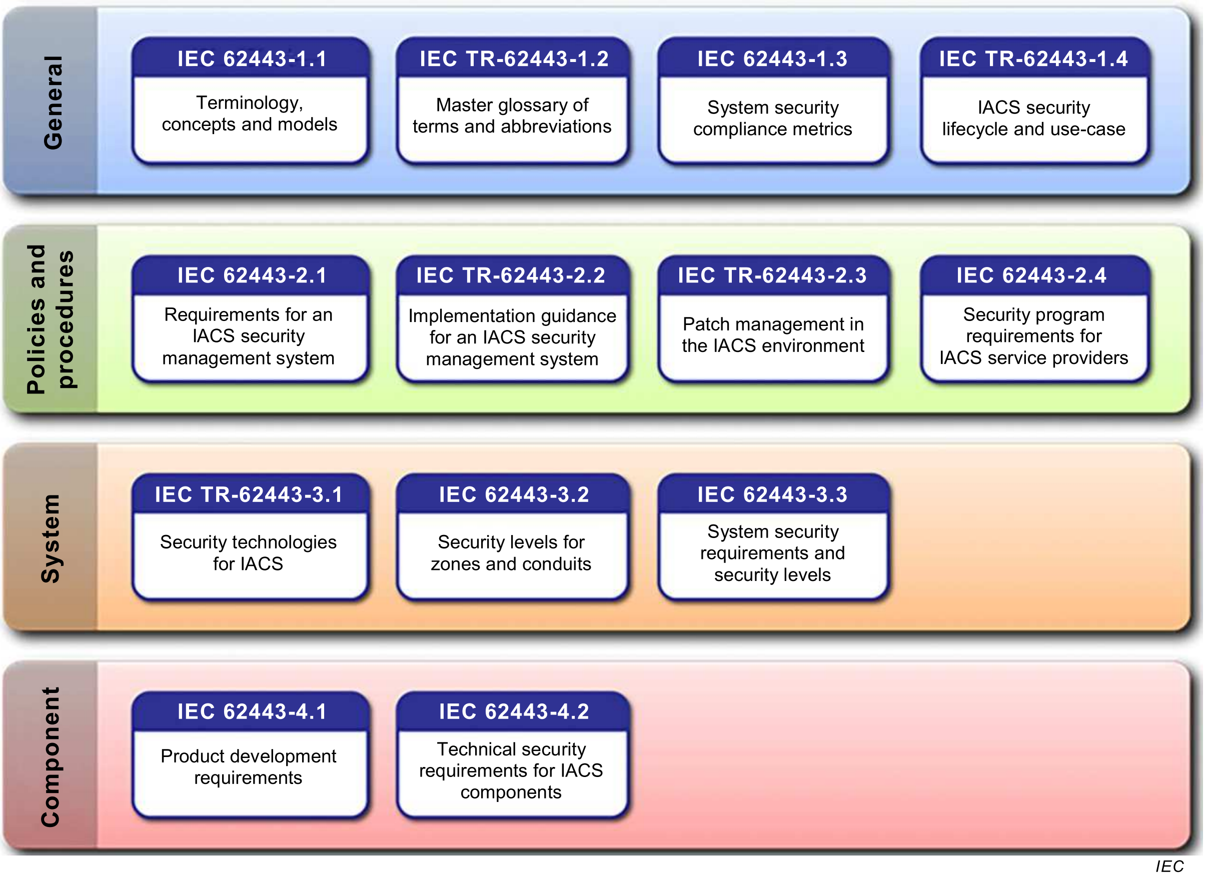

General
IEC 62443-1.1
Terminology, concepts and models
IEC TR-62443-1.2
Master glossary of terms and abbreviations
IEC 62443-1.3
System security compliance metrics
IEC TR-62443-1.4
IACS security lifecycle and use-case
Policies and procedures
IEC 62443-2.1
Requirements for an IACS security management system
IEC TR-62443-2.2
Implementation guidance for an IACS security management system
IEC TR-62443-2.3
Patch management in the IACS environment
IEC 62443-2.4
Security program requirements for IACS service providers
System
IEC TR-62443-3.1
Security technologies for IACS
IEC 62443-3.2
Security levels for zones and conduits
IEC 62443-3.3
System security requirements and security levels
Component
IEC 62443-4.1
Product development requirements
IEC 62443-4.2
Technical security requirements for IACS components
IEC

Figure 1 – Parts of the IEC 62443 Series

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

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

1 Scope

This part of IEC 62443 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.

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).

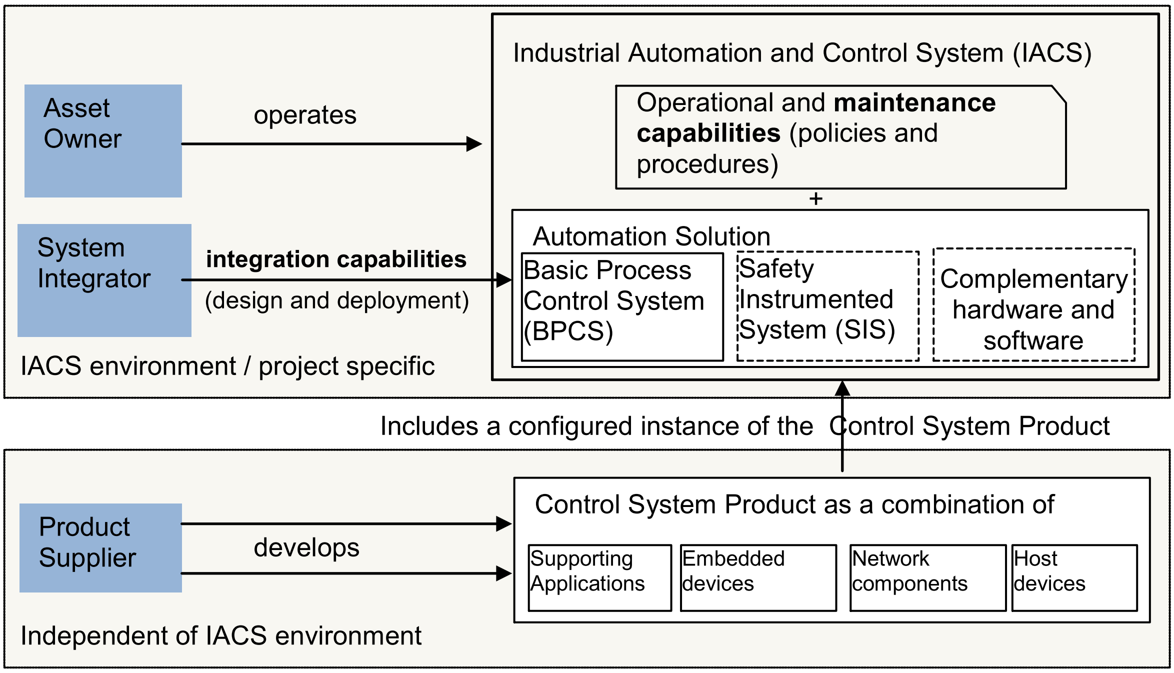

Asset Owner
operates
Industrial Automation and Control System (IACS)
Operational and maintenance capabilities (policies and procedures)
+
System Integrator
integration capabilities
(design and deployment)
Automation Solution
Basic Process Control System (BPCS)
Safety Instrumented System (SIS)
Complementary hardware and software
IACS environment / project specific
Includes a configured instance of the Control System Product
Product Supplier
develops
Control System Product as a combination of
Supporting Applications
Embedded devices
Network components
Host devices
Independent of IACS environment
IEC

Figure 2 – Scope of service provider capabilities

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

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

NOTE 4 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.

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.

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.

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.

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.

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

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.

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.

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”.

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.

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.

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.

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. 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 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		

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 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).

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

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 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.

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.

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

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

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.

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.

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

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 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 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.

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 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).

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 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.

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.

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.

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.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.01.04	BR	Solution staffing	Background checks	Service provider	No	The service provider shall have the capability to ensure that it assigns only service provider personnel to Automation Solution related activities who have successfully passed security-related background checks, where feasible, and to the extent allowed by applicable law.	The capabilities specified by this BR and its REs are used to protect the Automation Solution from being staffed with personnel whose trustworthiness may be questionable. While the background check cannot guarantee trustworthiness, it can identify personnel who have had trouble with their trustworthiness. Having this capability means that the service provider has an identifiable process for verifying the integrity of the service provider personnel it will assign to work on the Automation Solution. This requirement also recognizes that the ability to perform background checks is not always possible because of applicable laws or because of lack of support by local authorities and/or service organizations. For example, there may be countries that do not prohibit background checks, but that provide no support for conducting a background check, making it infeasible or impractical for the service provider to perform such a check. How and how often background checks are performed are left to the service provider. Examples of background checks include identity verification and criminal record checks.
SP.01.04	RE(1)	Solution staffing	Background checks	Subcontractor	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 successfully passed security-related background checks where feasible, and to the extent allowed by applicable law.	Having this capability means that the service provider has an identifiable process for verifying the integrity of the subcontractors, consultants, and representatives of the service provider who will be assigned to work on the Automation Solution. This requirement also recognizes that the ability to perform background checks is not always possible because of applicable laws or because of lack of support by local authorities and/or service organizations. For example, there may be countries that do not prohibit background checks, but that provide no support for conducting a background check, making it infeasible or impractical for the service provider to perform such a check. How and how often background checks are performed are left to the service provider. Examples of background checks include identity verification and criminal record checks. See ISO/IEC 27036-3 for additional supply chain organizational requirements.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.01.05	BR	Solution staffing	Personnel assignments	Security contact	No	The service provider shall have the capability to assign a security contact in its organization to the Automation Solution who is responsible and accountable for the following activities. 1) Acting as liaison with the asset owner, as appropriate, about the service provider's and the Automation Solution's adherence to the Part 2-4 requirements that are required by the asset owner. 2) Communicating the service provider's point-of-view on IACS security to the asset owner's staff. 3) Ensuring that tenders to the asset owner are aligned and in compliance with the Part 2-4 requirements specified as required by the asset owner and the service provider's internal IACS security requirements. 4) Communicating to the asset owner deviations from, or other issues not conforming with, the Part 2-4 requirements that are required by the asset owner. This includes deviations between these requirements and the service provider's internal requirements.	The capability specified by this BR is used to The capability specified by this BR is used to enhance security-related communication between the asset owner and the service provider to allow the service provider to be more responsive to Automation Solution security needs. Having this capability means that the service provider has an identifiable process for assigning a person to the Automation Solution who will be responsible for coordinating security related issues with the asset owner, such as deviations from the Part 2-4 and Part 3-3 requirements. Having a security contact provides the organizational vehicle for the asset owner to work with the service provider to address deviations from Part 2-4 capabilities and deviations of the control system used in the Automation Solution from Part 3-3 requirements (e.g. how to provide compensating mechanisms).

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.01.06	BR	Solution staffing	Personnel assignments	Security lead	No	The service provider shall have documented minimum IACS cyber-security qualifications for security lead positions and the capability to assign security leads to Automation Solutions who meet these qualifications.	The capability specified by this BR is used to reduce errors in security decision making and implementation. Making poor choices or lacking the ability to properly implement security can unnecessarily expose the Automation Solution to security threats and/or compromises. Having this capability means that the service provider has documented the qualifications (expertise/ competencies) that it requires of personnel who lead cyber-security related activities and has an identifiable process for staffing each Automation Solution with personnel who have this expertise. Expertise may include IACS cyber-security experience, training and certifications, and in general, the service provider and asset owner will typically come to agreement on the cyber-security qualifications for personnel before staffing begins. The phrase "meet these qualifications" is used to indicate that the security leads assigned to the Automation Solution have relevant experiences that confirm their compliance with these qualifications.
SP.01.07	BR	Solution staffing	Personnel assignments	Change	No	The service provider shall have the capability to notify the asset owner of changes in service provider, subcontractor, or consultant personnel who have access to the Automation Solution.	The capability specified by this BR is used to protect the Automation Solution against threats posed by service provider, subcontractor, and/or consultant personnel who no longer need access to the Automation Solution. Once notified of changes in personnel, the asset owner can update access authorizations accordingly (e.g. revoking badges, removing user accounts and associated access control lists). Having this capability means that the service provider has an identifiable process for notifying the asset owner of changes in service provider staffing. Timeliness of the notification and which personnel changes require notification are typical elements agreed to by the service provider and the asset owner. For example, service provider personnel who access the Automation Solution using temporary accounts may not be included since their temporary accounts will be removed when they are no longer needed.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.02.01	BR	Assurance	Solution components	Verification	Yes	The service provider shall have the capability to provide documentation that verifies that Automation Solution components identified by the asset owner (e.g. as result of a security assessment, threat analysis, and/or security testing) have adequate security for their level of risk.	The capability specified by this BR is used to provide confidence that components in the Automation Solution have security capabilities commensurate with their level of security risk. Having this capability means that the service provider has an identifiable process for confirming that Automation Solution components provide the appropriate level of security protections required by the asset owner. Security assessments and certifications, testing, and/or other methods may be used to provide this confirmation. Security testing refers to system or component testing whose primary objectives are to discover vulnerabilities and, conversely, to verify that specific attacks are handled as intended (e.g. mitigated, defeated, and/or diverted/quarantined). The success of security testing does not necessarily mean that the item under test is free from vulnerabilities. Examples of security tests include penetration tests, fuzz tests, robustness tests, and vulnerability scans. For related supply chain requirements, see IEC 62443-4-1, IEC 62443-4-2, and ISO 27036-3.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.02.02	BR	Assurance	Security tools and software	Technical description	Yes	The service provider shall have the capability to recommend security analysis tools (e.g. network scanning tools) for use with the Automation Solution and: 1) Provide instructions on how to use them, 2) Identify any known adverse effects they may have on the Automation Solution's performance, 3) Provide recommendations for how to avoid adverse effects.	The capabilities specified by this BR and its REs are used to ensure that the Automation Solution can be examined for security-related issues using asset owner approved tools. Security-related issues include the discovery of unauthorized devices on the network and/or unauthorized open ports on a device. Having this capability means that the service provider has an identifiable process for recommending one or more security analysis tools for the Automation Solution, along with information on potential problems their use may cause, and instructions for how to avoid these issues. This requirement directly implies that the service provider has to be aware of the potential problems a tool that it recommends might cause and report them to the asset owner along with recommendations for how to avoid them and how to use the tool effectively. Avoiding potential problems associated with the use of a tool may be accomplished by restricting configuration options, scheduling testing at opportune times, or by other means. For example, if it is known that a network scanning tool has the potential for overloading the network, then it might be configured to limit its impact on network traffic, or the network might be segmented to reduce the scope of overloads.
SP.02.02	RE(1)	Assurance	Security tools and software	Approval	No	The service provider shall have the capability ensure that it obtains approval from the asset owner prior to using security analysis tools (e.g. network scans) at the asset owner's site.	Having this capability means that the service provider has an identifiable process for coordinating the use of security analysis tools in the Automation Solution with the asset owner and receiving approval to use them. The BR for this RE requires the service provider to be able to inform the asset owner of potential adverse effects that these tools may have on the Automation Solution.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.02.02	RE(2)	Assurance	Security tools and software	Detection	No	The service provider shall have the capability to schedule and use security analysis tools to discover undocumented and/or unauthorized systems or vulnerabilities in the Automation Solution. This capability shall include the ability to use these tools in accordance with the asset owner's standard operating procedures.	Having this capability means that the service provider has an identifiable process for using tools to discover unauthorized devices connected to networks within the Automation Solution and other vulnerabilities, such as open ports that should not be open. Having this capability also means that the service provider has an identifiable process for coordinating and scheduling the use of security analysis tools to prevent them from impacting operations of the Automation Solution. The BR for this RE requires the service provider to inform the asset owner of potential adverse effects that these tools may have on the Automation Solution. Integration service providers are encouraged to schedule the use of these tools just prior to handover, for example, to find unauthorized devices and open ports, while maintenance service providers should use them regularly according to asset owner defined cycles. NOTE Where applicable, the network scans should look for devices on both wired and wireless network segments in the Automation Solution.
SP.02.02	RE(3)	Assurance	Security tools and software	Robustness	No	The service provider shall have the capability to ensure the control system components used in the Automation Solution have the ability to maintain operation of essential control system functions in the presence of system and/or network scans during normal operation.	Having this capability means that the service provider has an identifiable process for ensuring that the components of the Automation Solution's control system accessible by network scanning tools are capable of withstanding network scans. See IEC 62443-3-3 for the system capabilities related to network scans. Robustness testing is often used to demonstrate this assurance.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.02.03	BR	Assurance	Hardening guidelines	Technical description	Yes	The service provider shall have the capability to provide documentation to the asset owner that describes how to harden the Automation Solution.	The capabilities specified by this BR and its RE are used to provide the asset owner with details of the security mechanisms and configuration settings for the Automation Solution. This supports asset owner initiatives to provide governance and detailed knowledge of Automation Solution security, including integration of the Automation Solution with plant networks and systems. Having this capability means that the service provider has an identifiable process for delivering a hardening guide that describes how to harden the Automation Solution (install/configure the security features of the Automation Solution). This hardening guide is to include both architectural and configuration considerations, such as firewall placement (architectural) and firewall rules (configuration) and also considerations when installing new components into the Automation Solution. In general, the hardening of the Automation Solution will follow recommendations of a risk assessment performed on the Automation Solution (see SP.03.01.BR and its REs). NOTE Hardening guides provided by the suppliers of the control system and other components used in the Automation Solution may be included in or referenced by the service provider’s hardening guide.
SP.02.03	RE(1)	Assurance	Hardening guidelines	Verification	No	The service provider shall have the capability to verify that its security hardening guidelines and procedures are followed during Automation Solution related activities.	Having this capability means that the service provider has an identifiable process for ensuring that personnel and their subcontractors/consultants/representatives follow the hardening procedures required in SP.02.03 BR. Checklists are often used for this purpose.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.01	BR	Architecture	Risk assessment	Perform	No	The service provider shall have the capability to conduct a security risk assessment of the Automation Solution or contribute to (participate in) a security risk assessment conducted by the asset owner or its agent. NOTE 1 The asset owner may additionally require the service provider to document its assessment. The “Doc?” column is set to “No” because this is a requirement to have the capability to perform the assessment and not a requirement to provide documentation.	The capabilities specified by this BR and its REs are used to ensure that the service provider is capable of identifying and analyzing risks to support identification and remediation of security risks to the Automation Solution. Having this capability means that the service provider has an identifiable process for performing or contributing to a risk assessment. In some cases, the asset owner will require the service provider to conduct the assessment, while in other cases, to take an active role in an assessment conducted by the asset owner or by a third party under the direction of the asset owner. In an active role, the service provider might be asked to provide detailed knowledge of the Automation Solution and its components, information about threats and/or vulnerabilities, or otherwise assist in an assessment that has significant participation/contribution by the asset owner. For guidance on perfuming risk assessments, see IEC 62443-2-1 and IEC 62443-3-2. NOTE 2 Security risk assessments can be performed at any point in Automation Solution design and implementation to identify and manage security risks, but are often first performed prior to Automation Solution design to provide the basis for security design decisions, and then often repeated to ensure that security risks are kept current. NOTE 3 Risk assessment performed at the time of commissioning provides the asset owner a benchmark based on the achieved or as-built security system. NOTE 4 The output of the security risk assessment is a contractual matter between the service provider and the asset owner.
SP.03.01	RE(1)	Architecture	Risk assessment	Reporting	No	The service provider shall inform the asset owner of the results of security risk assessments that it performs on the Automation Solution, including risk mitigation mechanisms and procedures.	Having this capability means that the service provider has an identifiable process for reviewing risk assessments of the Automation Solution which it has performed and for informing the asset owner of security issues that were found, including recommendations for security mechanisms/procedures to address them.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.01	RE(2)	Architecture	Risk assessment	Verification	No	The service provider shall have the capability to verify that security architecture reviews and/or security assessment and/or threat analysis of the control system used in the Automation Solution have been conducted by a third party.	Having this capability means that the service provider can provide verification that the security of the control system used in the Automation Solution has been reviewed by a third party. Typically the review is done on the control system product under the direction of the control system supplier.
SP.03.02	BR	Architecture	Network design	Connectivity	No	The service provider shall have the capability to ensure that the physical network segmentation architecture used in the Automation Solution, including its use of network security devices or equivalent mechanisms, is implemented according to the Automation Solution design approved by the asset owner.	The capabilities specified by this BR and its REs are used to ensure the use of access controls between network segments within the Automation Solution and between the Automation Solution and external networks/communication links. Access controls protect network segments by restricting traffic flows between them. Restrictions are generally defined by rules that whitelist and/or blacklist traffic based on a number of factors including source addresses, destination addresses, and content (e.g. deep packet inspection). Having this capability means that the service provider has an identifiable process for ensuring that the Automation Solution networks have been segmented as specified and as approved by the asset owner. The location of the network segmentation points and their corresponding network security devices should be based on a risk assessment (see IEC 62443-3-2) and on the requirements in this standard (IEC 62443-2-4). As implementation progresses, having this capability also means that the service provider has an identifiable process for ensuring that design documents are updated so that they accurately reflect the Automation Solution architecture (see SP.06.01 BR).
SP.03.02	RE(1)	Architecture	Network design	Connectivity	No	The service provider shall have the capability to identify and document the network segments of the Automation Solution and their interfaces to other segments, including external networks, and for each interface designate whether it is trusted or untrusted.	Having this capability means that the service provider has an identifiable process for identifying all network segments of the Automation Solution, how they are interconnected, which of them provide external access to the Automation Solution, and for designating each connection point (interface to/from a segment) as trusted or untrusted. Untrusted interfaces are those that allow connections with untrusted devices in other segments/systems. Risk assessments as described in IEC 62443-3-2 can be used in the determination of trust and the use of zones to establish trust boundaries.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.02	RE(2)	Architecture	Network design	Connectivity	No	The service provider shall have the capability to ensure that interfaces of the Automation Solution that have been identified as untrusted are protected by network security devices or equivalent mechanisms, with documented and maintained security rules. At a minimum, the following shall be protected: 1) External interfaces 2) Level 2/Level 3 interfaces (see NOTE 2 below) 3) Interfaces between the BPCS and the SIS 4) Interfaces connecting wired and wireless BPCS networks 5) Interfaces connecting the BPCS to data warehouses (e.g. enterprise historians) NOTE 1 For some, responsibility for maintaining firewall rules and documentation transfers to the asset owner prior to or at Automation Solution turnover. In this case, the service provider’s role may be, as required by the asset owner, only to support verification that the firewall rules are accurate and up-to-date. NOTE 2 Depending on the Automation Solution, Level 2/Level 3 interfaces may be “External” interface.	Having this capability means that the service provider has an identifiable process for protecting the Automation Solution from external access and for controlling access between Level 2 and Level 3 (e.g. through the use of firewalls/firewall rules). Within the Automation Solution, having this capability also means that the service provider has an identifiable process for protecting BPCS interfaces using network security devices or equivalent mechanisms, and for providing the information necessary to create security rules that are used to grant/deny access to BPCS ports and applications. If the service provider supplies or is responsible for the network security device or the equivalent mechanism, then the required support includes being able to configure the network security device/mechanism as needed. Risk assessments (see IEC 62443-3-2) can be used to determine which interfaces require safeguarding.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.03	BR	Architecture	Solution components	Vulnerabilities	No	The service provider shall have capabilities for handling vulnerabilities that affect the Automation Solution, including its related policies and procedures. These capabilities shall address: 1) The handling of vulnerabilities newly discovered in the Automation Solution or in its related policies and procedures for which the service provider is responsible, and 2) The handling of publically disclosed vulnerabilities affecting the Automation Solution.	Having this capability means that the service provider has an identifiable process for assessing, reporting, and disposing of (e.g. recommending mitigations, preparing remediation plans) vulnerabilities related to the Automation Solution components for which the service provider is responsible. Typically, the process of identifying vulnerabilities includes event analysis and correlation (see SP.08.01 BR), risk assessment (see SP.03.01 BR and its REs), network scans and other automated methods (see SP.02.02 BR and its REs), and assurance (see SP.02.01 BR). Software patches that result from the disposition of vulnerabilities are considered to be security patches.
SP.03.03	RE(1)	Architecture	Network design	Vulnerabilities	Yes	The service provider shall have the capability to provide documentation to the asset owner that describes how to mitigate security weaknesses inherent in the design and/or implementation of communication protocols used in the Automation Solution that were known prior to Automation Solution integration or maintenance activities.	The capability specified by this BR is used to ensure that compensating mechanisms are used to address weaknesses in Automation Solution communications. Having this capability means that the service provider has an identifiable process for informing the asset owner about known communication weaknesses in the Automation Solution and how to mitigate them. For example, if the Automation Solution uses unencrypted protocols for the transfer of sensitive data, then the service provider should recommend security measures, such as lockable switches and physical security for communication links, to protect transmission of the data. NOTE The asset owner may also require the service provider, as part of its service agreement with the service provider or via a separate service agreement, to inform the asset owner of the discovery of additional weaknesses/mitigations discovered after the normal term of integration or maintenance activities.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.04	BR	Architecture	Network design	Network time	No	The service provider shall have the capability to ensure that time distribution/synchronization for the Automation Solution is performed from a secure and accurate source that uses a protocol that is commonly accepted by both the security and industrial automation communities.	The capability specified by this BR is used to ensure that timestamps are used in the Automation Solution and that they are generated and distributed from a reliable source. Timestamps are used in forensics when examining event logs. Having this capability means that the service provider has an identifiable process for integrating a network time source into the Automation Solution. The ability to provide the time source is not within the scope of this requirement. However, whether or not the service provider provides the time source, it is the responsibility of the service provider to integrate the time source into the Automation Solution. An example of a commonly accepted time source protocol IEEE 1588-2008/IEC 61588:2009.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.05	BR	Architecture	Devices – All	Least functionality	No	The service provider shall have the capability to ensure that only software and hardware features required by the Automation Solution or approved by the asset owner are enabled in the Automation Solution. At a minimum, this includes ensuring that: 1) unnecessary software applications and services (e.g. email, office applications, games) and their associated communication access points (e.g. TCP/.UDP ports), USB devices (e.g. mass storage), Bluetooth and wireless communications are disabled and/or removed unless required by the Automation Solution. 2) network addresses in use are authorized, 3) physical and logical access to diagnostic and configuration ports is protected from unauthorized access and use. 4) unused ports on network devices (e.g. switches and routers) are configured to prevent unauthorized access to the Automation Solution's network infrastructure. 5) maintenance processes maintain the hardened state of the Automation Solution during its lifetime.	The capabilities specified by this BR and its RE are used to limit access to the Automation Solution by removing/disabling unnecessary features and preventing unauthorized access to different types of Automation Solution interfaces (e.g. network device and configuration/diagnostic ports). Having this capability means that the service provider has an identifiable process for reducing the attack surface of the Automation Solution, for limiting access to the listed interfaces/ports to authorized users, and for maintaining the hardened state of the Automation Solution. This process may include the use of network security tools described in SP.02.02 BR and its REs. Limiting the software applications and their associated communication access points, USB devices such as mass storage devices, and wireless communications capabilities to only those necessary to perform the functions of a device used in both normal and emergency operations reduces the number of avenues into the device for an attack. Identifying unnecessary and/or unauthorized access points (e.g. using network scanning tools) is one technique that can be used to discover unnecessary software programs. Identifying network addresses that are unauthorized, for example using network scans as described in SP.02.02 RE(2), and removing them (e.g. by disconnecting the devices to which they are assigned) limits the source of passive and active attacks. Controlling access to physical configuration ports of devices, such as serial ports is intended to prevent or reduce the risk of having the network configuration (network devices) or the operation of other devices changed without proper authorization. Different methods for controlling access include installing a device in a locked cabinet, being able to physically lock the configuration port, or otherwise disabling use of the port when its use is not authorized (e.g. through a software lock).

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
							Locking down network device ports (switches and routers) reduces the possibility that an unauthorized device will be able to connect to the network and launch attacks or sniff the network. Control system products may have already removed capabilities unused by them prior to or during installation, making it necessary for the service provider to ensure that they are added/enabled only if they are required and approved by the asset owner. Maintenance processes provide the possibility that previously hardened components of the Automation Solution are reset or reconfigured to lose some aspect of their hardening. Controlling these processes reduce this possibility.
SP.03.05	RE(1)	Architecture	Devices – All	Least functionality	No	The service provider's hardening guidelines and procedures shall ensure that only necessary, authorized, and documented digital certificates for certificate authorities (CAs) are installed.	Having this capability means that the service provider has an identifiable process for determining which CA certificates are installed and removing those that are not used/authorized. Typically operating system installation and upgrades cause a generic set of Certificate Authority certificates to be installed, even though they are not required for the Automation Solution. Limiting which CA certificates are installed to only those that are necessary prevents authentication of unwanted, undesirable, or unnecessary applications.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.06	BR	Architecture	Devices – Workstations	Session lock	No	The service provider shall have the capability to support the use of session locking for Automation Solution workstations as required by the asset owner. This requirement applies only to the workstations for which the service provider is responsible. Session locking: 1) prevents information on the logged on user's display device from being viewed, and 2) blocks input from the user's input device (e.g. keyboard, mouse) until unlocked by the session user or an administrator. NOTE Locking the user input device means that the user at the workstation is not able to use the keyboard except for unlocking the keyboard.	The capability specified by this BR is used to ensure that workstations can be locked to protect against disclosure of information on the user's display device (e.g. screen) and against use of the user input device (e.g. keyboard, mouse). Having this capability means that the service provider has an identifiable process for enabling automatic screen locking for workstations, as required by the asset owner. Automatic screen locking causes the workstation screen to stop displaying and prevents data input until the authorized logged-on user unlocks the screen, typically by reentering the password. Which workstations need automatic screen locking enabled is defined by the site security requirements, which are often the result of a risk assessment (see IEC 62443-3-2). For example, workstations used to administer network devices and wireless networks are normally unattended and in accessible locations and therefore require automatic session locking enabled. This requirement only applies to workstations for which the service provider is responsible.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.07	BR	Architecture	Devices – Workstations	Access control	No	The service provider shall have the capability to ensure that wired and wireless workstations, including handhelds, used for maintenance and engineering of wired and wireless control/instrumentation devices do not circumvent the: 1) Automation Solution's access controls for these devices, 2) network security safeguards (e.g. network security devices) at the Automation Solution's boundary with Level 3. NOTE 1 Direct access to these devices by handhelds that bypass access controls of the Automation Solution is prohibited. NOTE 2 Direct access by a handheld to a wireless device in Level 3 that bypasses the Level 2/3 network security device is prohibited.	The capabilities specified by this BR and its RE are used to ensure that the Automation Solution's access controls (including authentication mechanisms) are always used to prevent unauthorized access to the Automation Solution's field devices from workstations/handhelds. Having this capability means that the service provider has an identifiable process for ensuring that there are no direct paths between workstations/handhelds and control/instrumentation devices that bypass the control system's access controls. The assumption is that access controls to these devices by engineers and operators is built into the control system. However, maintenance or engineering may be done using handhelds or other workstations that are not tightly integrated with the control system, and this required capability ensures that they cannot directly connect to control/instrumentation devices, bypassing the control system's access controls.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.07	RE(1)	Architecture	Devices – Workstations	Access control	No	The service provider shall have the capability to support the use of multi-factor authentication for Automation Solution workstations as required by the asset owner. This requirement applies only to the workstations for which the service provider is responsible.	Having this capability means that the service provider has an identifiable process for using multi-factor authentication in workstations as required by the asset owner. This support may include the ability to supply the necessary hardware and/or set up workstations to enforce multi-factor authentication. In practice, the type and level of authentication used for workstations will be defined by the site security requirements, which are often the result of a risk assessment (see IEC 62443-3-2). In general, multi-factor authentication is used for workstations that are accessible by personnel who are not authorized users of the Automation Solution, such as workstations that are normally unattended and/or in uncontrolled spaces. This requirement only applies to workstations for which the service provider is responsible. Multi-factor authentication includes, at a minimum, at least two of the following: 1) something the user knows, such as a password, 2) something the user possesses (a physical token), such as a smart card, 3) something inherent about the user, such as a retinal scan 4) someplace you are.
SP.03.08	BR	Architecture	Devices – Network	Least functionality	No	The service provider shall have the capability to ensure that least privilege is used for the administration of network devices for which the service provider is responsible.	This BR and its REs recognize that network devices are critical to the Automation Solution, and as a result, are often the subject of attack. Therefore, this BR and its REs are defined to ensure that the various facets of network device administration are protected. Having this capability means that the service provider has an identifiable process for applying the concept of least privilege to the administration of network devices. Least privilege for administrative operations means that access is granted only to resources (e.g. directories and files) that are needed and operating system privileges are similarly restricted to only those that are needed.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.08	RE(1)	Architecture	Devices – Network	Access control	No	The service provider shall have the capability to ensure that access controls used for the administration of network devices and wireless networks include role-based access controls. NOTE Normally network devices are only accessed by administrators so it is necessary to define only a single role for them. However, if the asset owner's operating procedures allow access to the network devices by administrators and others, then multiple roles can be defined.	Having this capability means that the service provider has an identifiable process for configuring network devices to use role-based access controls. Defining separate roles allows separate access control lists to be defined for each role, thus supporting the concept of least privilege. Normally, network devices are accessed only by administrators so only one role needs to be defined and the access control list to be set accordingly. However, if the asset owner's operating procedures provide for different levels of network device administration, then multiple roles need to be defined. Users capable of administering network devices will then be granted these roles. See IEC 62351-8 for further discussion of role based access controls.
SP.03.08	RE(2)	Architecture	Devices – Network	Cryptography	No	The service provider shall have the capability to ensure that encryption is used to protect data, whether in transit or at rest, that is used in the administration of network device (e.g. passwords, configuration data) that is identified as data requiring safeguarding (see SP.03.10 BR and its REs). NOTE See SP.03.10 RE(3) for cryptographic requirements.	Having this capability means that the service provider has an identifiable process for ensuring that data used for the administration of network device that is regarded as sensitive data as specified in SP.03.10 BR and its REs is protected by encryption within the device and on communication links. Encryption used on communications links can be performed at the network layer, on the transport layer connection, or at the message level to protect the data "on the wire". Encryption within network devices is used to prevent attacks on the configuration by malicious software in the device (e.g. as a result of hacking). The use of encryption mechanisms that provide integrity protection should be considered, such as AES_GCM.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.08	RE(3)	Architecture	Devices – Network	Access control	No	The service provider shall have the capability to ensure that access controls used for the administration of network devices include mutual authentication.	Having this capability means that the service provider has an identifiable process for configuring network devices to use mutual authentication. Mutual authentication validates the identity of the user and the network device, and results in the ability of the network device to determine whether the user is authorized to access the device, and in the ability for the user to ensure the device is the intended device and is not being spoofed. Challenge/response, user password/device certificate, and Kerberos (RFC 1510), are examples of techniques used to provide mutual authentication.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.09	BR	Architecture	Data protection	Communications	No	The service provider shall have the capability to ensure that the Automation Solution is configured to verify that all control actions and data flows in the Automation Solution (e.g. between workstations and controllers), including configuration changes, are: 1) valid, 2) initiated or approved by an authorized user, and 3) transferred over an approved connection in the approved direction.	The capability specified by this BR is used to ensure that there are manual and/or automated controls in place to prevent Automation Solution devices, such as controllers, from executing invalid and/or unauthorized commands. Having this capability means that the service provider has an identifiable process for ensuring that all commands (e.g. writes to setpoints, configuration commands) sent to Automation Solution devices (e.g. from workstations) are valid (within authorized limits), are authorized by a user with the appropriate permissions, and are transferred to the device executing the command (e.g. controller) over a connection that has been designated/authorized to be used for this purpose (e.g. a connection from an Operator Console to a controller). The intent of the second item of the requirement is to make sure that commands can only be requested by authorized users (e.g. operators), that the entity receiving and executing the command knows which connections are authorized for receiving commands, and that the command is checked for validity. Validity is normally value and state dependent. For example, a setpoint normally is not allowed to be written by the operator without putting the loop into manual control. This requirement also requires the service provider to have an identifiable process for ensuring that data flows are conducted over an authorized connection and that the data is transferred in the authorized direction. The intent of this portion of the requirement is make sure that the flow of data, including the direction, is authorized and conducted over authorized connections. For example, if a dynamic change (not a configuration change) to a set point is initiated by an entity not explicitly authorized to make the change, such as an advanced control application, then the system will notify the operator of the change and the operator is required to approve it before it can take effect. If the operator does not approve it, the set point does not change.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
							NOTE 1 This requirement generally applies to commands issued by workstations and sent to controllers, and not to commands sent from controllers to Level 1 devices. NOTE 2 Authorization of connections may be performed automatically by the control system and/or through appropriate configuration by the service provider (setting up network addresses/ports authorized to send commands. NOTE 3 Risk assessments (see IEC 62443-3-2) can be used to determine which connections are authorized to perform control actions. If warranted by the risk assessment, "dual approval" system capabilities (see IEC 62443-3-3) can be used to support this requirement. Dual approval refers to the system requiring two people to authorize actions that can result in serious impact to the iACS. NOTE 4 "Initiated or approved by" means, for example, that the Automation Solution can prevent remote operators from changing setpoints without approval by the local operator through the authorized connection. How this is implemented is Automation Solution dependent.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.10	BR	Architecture	Data protection	Sensitive data	Yes	The service provider shall have the capability to ensure that data storage points and data flows within the Automation Solution that require safeguarding, as defined or approved by the asset owner, are documented, including the security requirements for their safeguarding (e.g. confidentiality, integrity).	The capabilities specified by this BR and its REs are used to ensure that data stored and/or transferred in the Automation Solution that needs protection is documented and adequately protected. Typically both the asset owner and the service provider collaborate to identify control system data that needs protection (e.g. passwords, certificates, keys) and other data deemed worthy of protection by the asset owner (e.g. recipes). Having this capability means that the service provider has an identifiable process for identifying the data within the Automation Solution, either at rest or in transit, that requires protection and the type of protection required. The definition of data requiring safeguarding often contains site-specific criteria, and therefore, the asset owner should provide or at least approve the criteria. Data at rest can be in memory or in a storage device, and data in transit is data that is being transferred from one entity to another (a data flow). Examples of the types of data to be protected include (this list is not exhaustive): 1) legal or regulatory information 2) asset owner confidential data, including proprietary data (e.g. recipes) and data identified in NDAs or other contractual vehicles 3) configuration and operational data (e.g. commands and parameters) 4) system data, such as cryptographic materials (e.g. keys and certificates), access control lists, passwords, network device data, 5) audit and event logs, 6) backup data, 7) historical data, 8) data warehouses.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.10	RE(1)	Architecture	Data protection	Sensitive data	No	The service provider shall have the capability to ensure that data within the Automation Solution requiring safeguarding, as described in SP 03.10 BR, is protected from unauthorized disclosure or modification, whether at rest or in transit.	Having this capability means that the service provider has an identifiable process for ensuring that, after the sensitive data in an Automation Solution has been identified, the Automation Solution is enhanced as necessary to protect that data. Risk assessments (see IEC 62443-3-2) performed early in the project are often used in the identification of data requiring safeguarding. Protection mechanisms typically include: 1) mechanisms to protect against unauthorized memory dumps and network sniffing, 2) cryptographic mechanisms, including: a) encryption keys b) public key security infrastructure, c) digital signatures, d) data transport and message encryption, e) data base encryption.
SP.03.10	RE(2)	Architecture	Data protection	Data/event retention	Yes	The service provider shall have the capability to provide documentation to the asset owner that describes the retention capabilities provided by the Automation Solution for storing/archiving sensitive data. This documentation includes capacities, pruning and purging functions, retention timeouts, etc.	Having this capability means that the service provider has an identifiable process for documenting how the Automation Solution stores/archives sensitive data, such as historical data and events. This may include internal capabilities of the Automation Solution (e.g. data volumes/capacities) or may identify capabilities required to export historical data/events to a history archive. Historical data and events can be used during forensics and event analysis and correlation.
SP.03.10	RE(3)	Architecture	Data protection	Cryptography	No	The service provider shall have the capability to ensure that the cryptographic mechanisms used in the Automation Solution, including algorithms and key management/distribution/protection, are commonly accepted by both the security and industrial automation communities.	Having this capability means that the service provider is able to ensure that components of the Automation Solution that it provides uses current encryption technology that is generally accepted for use in IACSs.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.03.10	RE(4)	Architecture	Data protection	Sanitizing	No	The service provider shall have the capability to ensure that when it removes a component from the Automation Solution, all data in the component requiring safeguarding, as described in SP 03.10 BR, is permanently destroyed/deleted.	The capability specified by this BR is used to prevent sensitive data in a component/device that has been removed from the Automation Solution from being subsequently disclosed to anyone who may have access to the component after its removal. Having this capability means that the service provider has an identifiable process for ensuring that devices that are removed from active participation in the Automation Solution are sanitized of their confidential or sensitive data. Typically this can be done by destroying memory or clearing it a number of times to remove residual data. The number of times memory has to be cleared is dependent on the type of memory.
SP.04.01	BR	Wireless	Network design	Technical description	No	The service provider shall have the capability to ensure that its Automation Solution architecture documentation describing wireless systems is current in its description of the following. 1) Data exchange between a Level 1 network and wireless instrumentation, 2) Data exchange between a Level 2 network and a Level 3 network through a secure wireless link, 3) Security mechanisms that prevent an intruder from gaining access to the Automation Solution using the wireless system, 4) Security mechanisms that restrict access within the Automation Solution by workers with handheld wireless devices, 5) Where required, security mechanisms that provide protection for remote management of wireless systems. NOTE 1 The term "Level" refers to the position in the Purdue Reference Model as standardized by ISA 95 and IEC 62264-1 (see clause 5.3).	The capability specified by this BR is used to ensure that wireless networks are protected from being used to gain unauthorized access to the Automation Solution. Having this capability means that the service provider has an identifiable process for keeping current its wireless communications architecture documentation that includes data flows, security mechanisms, and the use of wireless bridges. NOTE 2 Zones and conduits as described in IEC 62443-3-2 are often used to define the security boundaries associated with wireless access to wired devices/workstations in the Automation Solution.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.04.02	BR	Wireless	Network design	Access control	No	The service provider shall have the capability to ensure that access to wireless devices is protected by authentication and access control mechanisms that are commonly accepted by both the security and industrial automation communities.	The capabilities specified by this BR and its RE are used to ensure that wireless devices and their communications are protected from unauthorized access. Having this capability means that the service provider has an identifiable process for providing or using commonly accepted authentication mechanisms and access control lists that prevent unauthorized access to wireless devices.
SP.04.02	RE(1)	Wireless	Network design	Communications	No	The service provider shall have the capability to ensure that wireless communications are protected by cryptographic mechanisms that are commonly accepted by both the security and industrial automation communities.	Having this capability means that the service provider has an identifiable process ensuring that networks used in the Automation Solution employ commonly accepted security mechanisms to protect access to their data during transmission. This includes wireless communications between wireless devices and wireless access points and between wireless access points and other wireless access point.
SP.04.03	BR	Wireless	Network design	Communications	No	The service provider shall have the capability to ensure that wireless protocols used in the Automation Solution are compliant with standards commonly used within the industrial security community and with applicable regulations.	The capabilities specified by this BR and its REs are used to provide confidence that wireless networks use protocols that have been vetted for use in industrial applications. Having this capability means that the service provider (1) uses a commonly accepted standard wireless technology in the Automation Solution and (2) has an identifiable process that ensures that the wireless technology used is compliant with local regulations.
SP.04.03	RE(1)	Wireless	Network design	Wireless network identifiers	No	The service provider shall have the capability to ensure that unique, Automation Solution-specific identifiers are used for wireless networks and that all wireless identifiers are descriptive acronyms that are not obviously associated with the asset owner's site.	The capability specified by this RE is used to provide confidence that wireless networks are configured to prevent easy identification (network identifiers are not obvious). Having this capability means that the service provider has an identifiable process for ensuring that each wireless network is assigned its own identifier (e.g. SSID) and that these identifiers do not allow an external listener to identify the physical wireless network, its location, or owner of the wireless network. If the identifier values are defined by the asset owner, the service provider's role is, if required, to provide guidance for their definition and/or review of the defined identifiers.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.04.03	RE(2)	Wireless	Network design	Connectivity	No	The service provider shall ensure that the Automation Solution's wireless devices that have IP addresses use static addressing and have dynamic address assignment mechanisms (e.g. DHCP) disabled.	The capability specified by this RE is used to provide confidence that wireless networks are configured to prevent: 1) the use of unauthorized device addresses, 2) DHCP exhaustion attacks (by disabling the use of DHCP). Having this capability means that the service provider has an identifiable process for ensuring that wireless device that have IP addresses cannot have their addresses changed by dynamic address assignment mechanisms.
SP.05.01	BR	SIS	Risk assessment	Verification	No	The service provider shall have the capability to verify that security architecture reviews and/or security risk assessments of the communications of the SIS used in the Automation Solution have been conducted and addressed.	The capability specified by this BR is used to provide confidence that security risks associated with the SiS are addressed. Having this capability means that the service provider can provide verification that the security of SIS communications, both internal and external, identified by risk assessments/security reviews have been addressed. Typically the review is done on integrated SIS/control system product under the direction of the control system supplier in response to IEC 61511-1 Clause 8.2.4, and addressed by the supplier. In some cases, mitigation of risks is deferred to the service provider as part of the installation/maintenance of the Automation Solution. In these cases, this requirement requires the service provider to ensure the appropriate mitigations for the Automation Solution are determined and implemented.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.05.02	BR	SIS	Network design	Communications	No	The service provider shall have the capability to ensure that SIS safety communications and SIS safety functions are protected from the BPCS or any other Automation Solution communications. NOTE This requirement does not require that communications not critical to safety functions between the SIS and the BPCS (e.g. configuration downloads, status monitoring, logging) be shielded from other Automation Solution communications.	The capability specified by this BR is used to ensure that SIS communications critical to safety functions cannot be affected by other communications of the Automation Solution. Having this capability means that the service provider is able to protect or isolate SIS communications critical to safety functions from other Automation Solution traffic (see IEC 61508), for example, through the physical separation of BPCS communications and the SIS. In this example, firewalls and non-routable interfaces between the BPCS and SIS could be used to enforce this separation. Having this capability also means the service provider can demonstrate that the countermeasures taken to isolate functional safety communications do not impact the performance or operation of communications critical to safety. Risk assessments, zones (network segments), and conduits (connections between network segments), as described in IEC 62443-3-2, can be used in the definition of requirements.
SP.05.03	BR	SIS	Network design	Communications	No	The service provider shall have the capability to ensure that communications external to the Automation Solution, including remote access communications, are not able to interfere with the operation of the SIS.	The capability specified by this BR is used to ensure that the operation of the SIS cannot be impacted by communications of devices/applications external to the Automation Solution. SP.05.02 BR requires capabilities to protect SIS communications from other Automation Solution communications, while this requirement requires capabilities to protect the operation of the SIS from communications external to the Automation Solution. Having this capability means that the service provider has an identifiable process for ensuring that the operation of the SIS cannot be affected by communications of external applications, including remote access communications such as RDP.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.05.04	BR	SIS	Network design	Communications	No	The service provider shall have the capability to ensure that applications, (e.g. control system applications) external to the SIS are not able to participate in or disrupt or otherwise interfere with SIS communications that are critical to safety functions.	The capability specified by this BR is used to ensure that the SIS cannot be impacted by devices/applications external to the SIS. SP.05.03 BR requires capabilities to protect the SIS from communications external to the Automation Solution, while this requirement requires capabilities to protect SIS communications from interference by applications external to the SIS. Having this capability means that the service provider has an identifiable process for ensuring that there are no communications critical to safety functions (e.g. data and/or commands) transferred between the SIS and applications residing external to the SIS. This requirement is intended to prevent the SIS functions critical to safety operations from being compromised by traffic originating from sources outside the SIS.
SP.05.05	BR	SIS	Devices – Workstations	Communications	No	The service provider shall have the capability to ensure that SIS EWSs that reside outside the SIS (external to SIS interface with the control system) cannot be compromised by communications from Level 3 or above. NOTE The term "Level" refers to the position in the Purdue Reference Model as standardized by ISA 95 and IEC 62264-1 (see 5.3).	The capability specified by this BR is used to employ safeguards, such as network security devices, to ensure that only authorized communications from Level 3 applications to SIS engineering workstations residing outside the SIS are permitted. Access from Level 3 applications to SIS engineering workstations that reside within the SIS is prohibited by SP.05.03 BR. Having this capability means that the service provider has an identifiable process for ensuring that all communications between the SIS engineering workstation and Level 3 (and above) applications pass through a network security device, or equivalent mechanism, that connects Level 2 and Level 3 (or above).

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.05.05	RE(1)	SIS	Devices – Workstations	Communications	No	The service provider shall have the capability to ensure that the Automation Solution's SIS EWS that reside within the SIS (internal to SIS interface with the control system) cannot be compromised by remote access (e.g. RDP).	The capability specified by this RE is defined to be able to protect SIS engineering workstations that reside inside the SIS from being exploited via remote access connections. See SP.05.05 BR that addresses access from Level 3 to SIS EWSs external to the SIS. Having this capability means that the service provider has an identifiable process for ensuring that SIS engineering workstations within the SIS (1a) either do not have remote access installed or (1b) have it disabled (not accessible), and/or (2) have security mechanisms that block remote access communications with these workstations. NOTE See IEC 62443-3-2 for guidance on what to consider in such risk assessments from a cyber-security perspective.
SP.05.06	BR	SIS	Devices – Workstations	Connectivity	No	The service provider shall have the capability to ensure that all access to the Automation Solution's SIS from outside the SIS is mediated and authorized at the interface to the SIS.	The capability specified by this BR is used to limit the number of physical access paths to the SIS, and hence reduce its attack surface. Having this capability means that the service provider has an identifiable process for ensuring that access controls to the SIS are implemented at the interface to the SIS, for example by a gateway used only to provide access to the SIS from the BPCS. Implementation of this gateway may be provided by the BPCS or the SIS.
SP.05.07	BR	SIS	Devices – Workstations	Least functionality	No	The service provider shall have the capability to ensure that SIS functions performed by the Automation Solution's SIS EWS are protected from compromise by other SIS EWS software.	The capability specified by this BR is used to reduce the possibility that the SIS EWS will contain T3 offline software (see IEC 61508-3) that could intentionally or inadvertently cause harm to the SIS. Having this capability means that the service provider has an identifiable process for ensuring that safety-related software running in SIS EWSs is protected from compromise from other software running in the SIS EWS.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.05.08	BR	SIS	Devices – Wireless	Connectivity	No	The service provider shall have the capability to verify that unauthorized wireless devices are not used as an integral part of SIS safety functions.	The capability specified by this BR is used to prevent attacks against the SIS by unauthorized wireless devices. Since wireless devices are not bounded by physical security perimeters nor by physical implementation, they can present a threat to the SIS. Having this capability means that the service provider has an identifiable process for verifying that wireless device communications are not used as an integral part of SIS safety functions when prohibited by the asset owner. “Integral part” refers to communications that are implemented and incorporated into SIS safety functions. See SP.04.01 BR for requirements for the general use of wireless technologies within the Automation Solution.
SP.05.09	BR	SIS	User interface	Configuration mode	No	The service provider shall have the capability to ensure that SIS configuration mode can be enabled and disabled. While disabled, this interface shall prohibit the SIS from being configured. NOTE This interface will typically prevent configuration messages from being delivered to the SIS.	The capabilities specified by this BR and its REs are used to prevent configuration access to the SIS during normal operation through a mechanism that requires the SIS to be unlocked to configure it, and locked at all other times. Having this capability means that the service provider is able to ensure that the SIS can be locked to prevent configuration changes from being made and unlocked to allow them to be made. Locks can be physical key switches or software controlled locks, but however implemented they allow the SIS to be locked to prevent inadvertent or malicious changes from being made.
SP.05.09	RE(1)	SIS	User interface	Configuration mode	No	The service provider shall have the capability to provide a hardware implementation of the configuration mode interface required by SP.05.09 BR and to ensure that this hardware implementation is capable of being physically locked while configuration mode is disabled.	The capability specified by this RE is defined to require intentional human intervention to enable configuration of the SIS, such as holding a physical key open (unlocked) while the configuration is being changed, for the purpose of increasing confidence that inadvertent changes to the SIS configuration cannot occur. Having this capability means that the service provider is able to ensure that the SIS has a hardware interface that can be disabled to prevent configuration changes from being made. The hardware interface, such as a physical key switch, when physically locked (e.g. removing the key), configuration mode is disabled.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.05.09	RE(2)	SIS	User interface	Configuration mode	No	The service provider shall have the capability to have an independent 3rd party verify that it is not possible to change the configuration of the SIS when the hardware interface described in SP.05.09 RE(1) is locked in the "disable" configuration mode.	The capability specified by this RE is defined to add an additional level of confidence that the physical locking mechanism works as intended. Having this capability means that the service provider has an identifiable process for providing a report from a 3rd party that verifies that the SIS configuration locking mechanism works. This report may be initiated (e.g. contracted) by the control system supplier for the Automation Solution or by the service provider. This verification may occur prior to delivery of the product to the Automation Solution (as part of product verification) or after delivery of the hardware interface (as part of the service provider's its Automation Solution activities).
SP.06.01	BR	Configuration management	Network design	Connectivity	No	The service provider shall have the capability to provide accurate logical and physical infrastructure drawings/documentation of the Automation Solution, including its network devices, internal interfaces, and external interfaces. The documentation and drawings shall be maintained as an accurate representation of the Automation Solution.	The capabilities specified by this BR and its RE are used to ensure that an accurate representation of the Automation Solution network architecture is documented and available for security-related activities, such as risk assessments and forensic analysis. Having this capability means that the service provider has an identifiable process for keeping its network architecture documentation current. The network architecture includes each network segment, the network devices used to interconnect the network segments, and an identification of all network interfaces internal to the Automation Solution and those that connect the Automation Solution to external networks. Network interfaces can be identified through a variety of techniques, including Ethernet addresses (i.e. MAC addresses), IP addresses, and network interface card identifiers. The intent is to provide enough information about them to unambiguously identify them. Risk assessments, zones (network segments), and conduits (connections between network segments), as described in IEC 62443-3-2, can be used in the development of the network architecture.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.06.01	RE(1)	Configuration management	Network design	Connectivity	No	The service provider shall have the capability to keep the as-built and installed equipment connection and configuration documents current.	Having this capability means that the service provider has an identifiable process for keeping its documentation up-to-date that describes the devices connected to each network segment in the Automation Solution. EXAMPLE For an Ethernet device, the documentation would include the network address and switch to which the device is connected, and a copy of the download file used to configure the device.
SP.06.02	BR	Configuration management	Devices – All	Inventory register	No	The service provider shall have the capability to create and maintain an inventory register, including version numbers and serial numbers, of all devices and their software components in the Automation Solution for which the service provider is responsible.	The capability specified by this BR is used to ensure that a component inventory is maintained to make it possible to determine if a component in the Automation Solution is authorized, and also to be able to determine if a vulnerability newly discovered within the industry is applicable to the Automation Solution. For example, if a vulnerability to a specific version/patch level is discovered, it should be possible to consult the Automation Solution inventory to determine if the vulnerability is applicable to devices/components used in the Automation Solution. Having this capability means that the service provider has an identifiable process for providing documentation for all components of the Automation Solution for which it is responsible. Characteristics include information such as model numbers, version numbers, and serial numbers. Documentation may include reports, automatically generated configuration data, screen captures, etc.
SP.06.03	BR	Configuration management	Devices – Control and instrumentation	Verification	No	The service provider shall have the capability to verify that wired and wireless devices used for control and instrumentation have been configured correctly with their approved values.	The capability specified by this BR is used to verify the integrity of device configurations. The intent is to be able to detect unauthorized or erroneous configuration changes. Having this capability means that the service provider has an identifiable process for verifying that device configuration parameters values have been correctly downloaded/written to the device. EXAMPLE Configuration parameter values can be confirmed by viewing them from a workstation.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.07.01	BR	Remote access	Security tools and software	Connectivity	No	The service provider shall have the capability to ensure that all remote access applications used in the Automation Solution are commonly accepted by both the security and industrial automation communities.	The capability specified by this BR is used to ensure that remote access applications provide acceptable levels of protection to the Automation Solution. Having this capability means that the service provider has an identifiable process for ensuring that all remote access applications are supported by commonly accepted remote access mechanisms (e.g. RDP). Remote access clients may be provided by the client and/or the service provider.
SP.07.02	BR	Remote access	Security tools and software	Technical description	No	The service provider shall have the capability to provide detailed instructions for the installation, configuration, operation, and termination of the remote access applications used in the Automation Solution.	The capability specified by this BR is used to ensure that remote access applications provide acceptable levels of protection to the Automation Solution. Having this capability means that the service provider has documentation for installing, configuring, and operating remote access applications that it recommends for use in the Automation Solution. The service provider is also required to provide instructions to the asset owner for the termination of these connections. The service provider is not permitted to establish remote access connections that cannot be terminated by the asset owner.
SP.07.03	BR	Remote access	Security tools and software	Technical description	No	The service provider shall have the capability to provide information about all proposed remote access connections to the asset owner that includes, for each connection: 1) its purpose, 2) the remote access application to be used, 3) how the connection will be established (e.g. via the Internet through a VPN), and 4) the location and identity of the remote client.	The capability specified by this BR is used to ensure that remote access to the Automation Solution is documented and managed to thwart unauthorized attempts to gain remote access to the Automation Solution. Having this capability means that the service provider has an identifiable process for defining and informing the asset owner of the details of all proposed remote access connections. The proposed location of the remote access client is required to be documented to allow the asset owner to review and approve/disapprove remote access from specific locations. In some cases, the proposed location may indicate “roaming” to allow for portable devices to be used as clients. It is not anticipated that the Automation Solution can automatically verify the physical location of the client at runtime.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.07.04	BR	Remote access	Security tools and software	Approval	No	The service provider shall have the capability ensure that it obtains approval from the asset owner prior to using each and every remote access connection.	The capability specified by this BR is used to ensure that all remote access connections to the Automation Solution are authorized by the asset owner. Having this capability means that the service provider has an identifiable process for using only those connections that have been approved by the asset owner. These remote access connections may be user-to-system or system-to-system, may traverse the Internet and/or include the use of modems, and/or may be provided and maintained by the asset owner. Requirements for management of these connections and the time needed by the asset owner to approve the connections are beyond the scope of this requirement. In addition, the asset owner may request the service provider to provide or maintain the connections and may provide the appropriate requirements at that time. For example, the asset owner may not allow TCP/IP protocols to be used over external connections that use modems. A risk assessment, as described in IEC 62443-3-2, may be used to define these requirements, including whether or not the connection should be encrypted, and whether or not a modem can be used to provide the connection, and if so, whether the modem should be disconnected when not in use, and whether the modem should be capable of being used as a router.
SP.07.04	RE(1)	Remote access	Data protection	Cryptography	No	The service provider shall have the capability to ensure that all remote access connections conducted over the Internet or over other publically accessible media that are used to support remote access to the Automation Solution by the service provider (e.g. from a service provider facility) are authenticated and encrypted.	The capability specified by this RE is defined to ensure that all connections used to support remote access to the Automation Solution by the service provider are protected. Service providers often offer remote support and troubleshooting/diagnostic services to the Automation Solution. Having this capability means that the service provider has an identifiable process for using encrypted links, such as VPNs, for remote access to the Automation Solution over the Internet by the service provider (e.g. from its facilities or other remote locations). Authentication is required to ensure that only authorized remote clients have access to the Automation Solution. In general, this requirement addresses the need for remote access to the Automation Solution by the service provider to support activities such as remote support.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.08.01	BR	Event management	Events – Security compromises	Responding	No	The service provider shall have capabilities for handling cyber-security incidents that affect the Automation Solution that include: 1) detecting cyber-security compromises and incidents, 2) reporting cyber-security incidents to the asset owner, 3) responding to cyber-security compromises and incidents, including supporting an incident response team. NOTE 1 Logging of security-related events is addressed by SP.08.02 BR. NOTE 2 Logging and reporting of alarms and events is addressed by SP.08.03 BR.	The capabilities specified by this BR and its REs are used to ensure that security incidents relevant to the Automation Solution are managed from detection through disposition to allow the security risk position of the Automation Solution to be maintained. Having this capability means that the service provider has an identifiable process for detecting, handling and reporting cyber-security incidents for Automation Solution components for which the service provider is responsible. What constitutes an incident, which incidents are significant, and under what conditions they are reported to the asset owner are all part of the service provider's incident handling procedures. Incident handling implementation may be controlled by specific agreements between the asset owner and service provider, such as non-disclosure agreements and/or other contractual vehicles between the asset owner and service provider. These contractual vehicles often identify proprietary data to be protected and the types of compromise that to be reported. Typically, the process of identifying incidents includes (1) event analysis and correlation, and (2) examination and triage of resulting compromises and potential incidents to yield incidents. SP.03.03 BR addresses handling of vulnerabilities that may have been exposed by this process or by other processes. In many cases, recognition that a compromise has occurred and that an associated loss has resulted can be difficult and may involve subjectivity and judgment. The specification of this process and the precise definition of what constitutes an incident is beyond the scope of these requirements. For requirements related to product development incident reporting and handling that can complement the service provider's incident handling capabilities, see IEC 62443-4-1 and ISO/IEC 30111.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.08.01	RE(1)	Event management	Events – Security compromises	Reporting	No	The service provider shall have the capability to ensure that security compromises that have been automatically detected can be reported through a communications interface that is accessible to the asset owner and that is commonly accepted by both the security and industrial automation communities.	Having this capability means that the service provider has an identifiable process for reporting security compromises in security that it detects automatically. Security compromises are to be reported whether or not they result in a loss or are classified as an incident. Security compromises can be automatically detected at the time of compromise or through subsequent event analysis and correlation activities (e.g. through the use of a Security Information and Event Management (SIEM) package).
SP.08.02	BR	Event management	Events – Security-related	Logging	No	The service provider shall have the capability to ensure that the Automation Solution is configured to write all security-related events, including user activities and account management activities, to an audit log that is kept for the number of days specified by the asset owner. NOTE Logging and reporting of process-related events, such as setpoint changes and other operational/configuration data changes, is addressed by SP.08.03 BR.	The capabilities specified by this BR and its REs are used to ensure that security-related audit logs are supported. Audit logs can be used in forensics (e.g. who changed a user account and when) and in event correlation activities that may lead to security incident identification. Audit logs require a higher level of integrity protection than provided by typical event logs. They are used to protect against claims that repudiate responsibility for an action. Having this capability means that the service provider has an identifiable process to provide audit logging for security-related events that include successful and invalid logins and logouts, and creation, modification or deletion of user accounts, among others.
SP.08.02	RE(1)	Event management	Events – Security-related	Reporting	No	The service provider shall have the capability to ensure that security-related data and events can be accessed through one or more interfaces that is/are commonly accepted by both the security and industrial automation communities.	Having this capability means that the service provider has an identifiable process for ensuring that it is possible for the asset owner to collect security data and events over the network. Commonly accepted interfaces include interfaces that support polling (SNMP reads), asynchronous reporting (e.g. SNMP traps), and logging (e.g. Syslog, Syslog-ng and Common Event Format (CEF)). Use of commonly accepted interfaces make it easier to integrate off-the-shelf software packages that collect and analyze data and events. EXAMPLE Network devices typically maintain an SNMP Management Information Base (MIB) that contains security-related data that can be accessed using SNMP.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.08.02	RE(2)	Event management	Events – Security-related	Logging	No	The service provider shall have the capability to verify that, using a simulated security-related event approved by the asset owner, security-related events can be written to an audit log.	Having this capability means that the service provider has an identifiable process for verifying that the mechanisms used to log and report security-related events operate as required by SP 08.02 BR and SP 08.02 RE(1). Audit logs require a higher level of integrity protection than provided by typical event logs. They are used to protect against claims that repudiate responsibility for an action.
SP.08.03	BR	Event management	Events – Alarms & Events	Logging	No	The service provider shall have the capability to ensure that the Automation Solution is configured to log and notify the operator of process-related events as required by the asset owner. The types of events include state changes/operating condition changes/configuration changes that may be due to manual or automated (those without human intervention) operation. NOTE 1 Logging of security-related events is addressed by SP.08.02 BR.	The capabilities specified by this BR and its RE are used to ensure that process-related event logs are supported. Event logs can be used in forensics (e.g. who changed a setpoint and when) and in event correlation activities that may lead to security incident identification. Having this capability means that the service provider has an identifiable process for ensuring that the Automation Solution supports logging and notification of process-related events, and for configuring it to log and notify operators of events designated by the asset owner. Notifications include both simple event notifications and alarm/alert notifications. Alarms and events to be logged and reported include both operating system events and control system alarms and events. Events reported through this interface may be determined to require safeguarding as required by risk assessment, (see SP.03.01 BR and its REs). See also SP.03.10 BR and its REs for requirements for the protection of sensitive data. NOTE 2 Alarms and alerts, as defined by ISA 18.2 or NAMUR NA102, are notifications that require operator response (alarm) or awareness (alert).
SP.08.03	RE(1)	Event management	Events – Alarms & Events	Reporting	No	The service provider shall have the capability to ensure that alarms/alerts/events can be securely reported through an interface that is commonly accepted by both the security and industrial automation communities.	Having this capability means that the service provider has an identifiable process for ensuring that the Automation Solution is able to report alarms and events to external applications, such as a centralized log, through a commonly accepted interface that protects the transmitted events against tampering and disclosure. This interface may support event notifications or event polling.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.08.04	BR	Event management	Events – Alarms & Events	Robustness	Yes	The service provider shall have the capability to document the Automation Solution’s ability to withstand the near-simultaneous occurrence of large numbers of events, typically referred to as event storms.	The capability specified by this BR is used to document the limits of the Automation Solution’s ability to protect against denial of service during event storms. The characteristics of event storms (e.g. number of events/second) are typically dependent on the number of control and instrumentation devices in the Automation Solution and the nature of the physical process. Having this capability means that the service provider has an identifiable process for providing documentation that describes the limits of the Automation Solution’s ability to handle event storms. Robustness testing and stress testing are often used to demonstrate this assurance.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.09.01	BR	Account management	Accounts – User and service accounts	Administration	No	The service provider shall have the capability to ensure that the Automation Solution supports: 1) the use of a single, integrated data base, which may be distributed or redundant, for defining and managing user and service accounts, , 2) restricted management of accounts to authorized users, 3) decentralized access to this data base for the management of accounts, 4) decentralized enforcement of the account settings (e.g. passwords, operating system privileges, and access control lists) defined in this data base.	The capability specified by this BR is used to simplify the management of user accounts for Automation Solutions composed of multiple workstations and servers. Without such capabilities, separately managing accounts across individual workstations and servers often results in inconsistencies that result in denial of service to resources and/or the inappropriate granting of access to resources. Having this capability means that the service provider is able to ensure that the Automation Solution provides an account management system that: 1) has a single data base that may be distributed or redundant, as determined by Automation Solution requirements, 2) allows accounts, including user, administrator/super user accounts, and service accounts (i.e. accounts that do not provide for interactive login), to be defined and managed only by authorized users, 3) allows administrators to manage accounts from a specified set of workstations/servers in the Automation Solution, not just from a single dedicated workstation, 4) distributes the enforcement of account access control lists and privileges to the location where the access or privilege is to be executed. Examples of this type of account management include Lightweight Directory Access Protocol (LDAP) based technologies such as Windows Active Directory. See IEC 62443-3-3 for related security requirements for systems used in Automation Solutions.
SP.09.02	BR	Account management	Accounts – User and service accounts	Administration	No	The service provider shall have the capability to ensure that unique accounts can be created and maintained for users.	The capability specified by this BR is used to prevent users from having to share accounts, i.e. by having a separate account. Having this capability means that the service provider has an identifiable process for creating and maintaining a unique user account for each Automation Solution user.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.09.02	RE(1)	Account management	Accounts – User and service accounts	Technical description	Yes	The service provider shall provide documentation to the asset owner that: 1) identifies all default user and service accounts, 2) describes the tools and procedures used to set/reset passwords for all default user and service accounts.	The capability specified by this RE is defined to ensure there are no hidden accounts nor are there passwords that cannot be changed. Having this capability means that the service provider has an identifiable process for generating a list of all user and service accounts and providing instructions to the asset owner that describes how to change their passwords. For accounts used by services and servers (e.g. DCOM server), changing a password may involve one or more of the following: 1) changing the password for the account, 2) changing the "logon" password in the services/services that run under the account, 3) changing the password used by other software processes that connect to other processes using the account.
SP.09.02	RE(2)	Account management	Accounts – User and service accounts	Administration	No	The service provider shall have the capability to ensure that if an account/password is automatically generated for a user, other than operators and service groups, both the generated account and password are unique.	The capability specified by this RE is defined to ensure that the same password is not generated for multiple user accounts, other than for operator and service groups. Having this capability means that the service provider has an identifiable process for verifying that the Automation Solution does not generate the same password for two different users and that each generated user account is unique and has a unique identifier. This requirement does not apply to Automation Solutions that do not generate accounts and passwords for individual users.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.09.02	RE(3)	Account management	Accounts – User and service accounts	Expiration	No	The service provider shall have the capability to ensure that service, auto-login and operator accounts, and other accounts required for essential functions and/or continuous operations, or as required by the asset owner have been configured so that they never expire nor become disabled automatically.	The capability specified by this RE is defined to prevent services, operators, workstations configured for auto-login, and other accounts as required, from experiencing denial of service because their accounts have expired or become automatically disabled. Having this capability means that the service provider has an identifiable process for ensuring that accounts that are permanent accounts in the Automation Solution, such as service, auto-login and operator accounts, are configured so that they do not expire or become automatically disabled or deleted. Operator accounts are typically individual user accounts configured with operator privileges that provide visibility into the physical environment (e.g. the process) being controlled. This requirement does not prevent permanent accounts from being removed, or otherwise disabled, based on explicit actions taken by an administrator. A commonly recommended measure for Unix-based systems is to configure the root account to use the false or “nologin” shell (and thus effectively denying all logins using this account) and creating a differently named alias for the root account for use by authorized administrative users. NOTE See SP.03.01 BR and its REs for assessing and addressing risks associated with accounts that do not expire.
SP.09.02	RE(4)	Account management	Accounts – Administrator	Least functionality	No	The service provider shall have the capability to ensure that the built-in administrator account is disabled, and if that is not possible, that it is renamed or otherwise made difficult to exploit.	The capability specified by this RE is defined to make it difficult for attackers to gain administrative privileges using the built-in administrator account. Having this capability means that the service provider has an identifiable process for disabling or renaming the built-in administrator account, or if neither of those is possible, making it difficult to recognize and exploit it. Providing access to the built-in administrator account allows malware to potentially use this account and gain control of the system. NOTE Renaming is not as effective since the operating system may not change the underlying identifier for the account.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.09.03	BR	Account management	Accounts – Default	Least functionality	No	The service provider shall have the capability to ensure that unused system default accounts have been removed or disabled.	The capability specified by this BR is used to prevent attackers from gaining access to the Automation Solution through unused system default accounts. Having this capability means that the service provider has an identifiable process for removing system default (built-in) accounts that are not needed for the Automation Solution. Built-in accounts are generally installed when new computers (e.g. workstations) are added to the Automation Solution or when their software is installed or reinstalled. This requirement applies to all default system accounts, whether they are installed with the operating system or with control system or related software. The service provider needs to have a process for ensuring unnecessary built-in accounts are removed.
SP.09.04	BR	Account management	Accounts – User	Least functionality	No	The service provider shall have the capability to ensure that all user accounts are removed once they are no longer needed. This includes: 1) temporary accounts under the control of the service provider, such as those used for integration or maintenance, 2) user accounts for service provider personnel who are no longer assigned to the Automation Solution (see SP.01.07 BR for notifying the asset owner of the removal of service provider personnel from the Automation Solution.	The capabilities specified by this BR and its RE are used to prevent attackers from gaining access to the Automation Solution through accounts that are not needed (e.g. accounts of users who are no longer assigned to the Automation Solution). Having this capability means that the service provider has an identifiable process for removing or disabling accounts that were created to support its personnel once their activities are complete or their assignment to the Automation Solution has ended. The intent is to ensure that the Automation Solution does not contain or retain service provider accounts unless they are needed.
SP.09.04	RE(1)	Account management	Accounts – User	Logging	No	The service provider shall have the capability to generate an audit log report after the completion of integration/maintenance activities that shows that accounts used to support these activities have been removed from the Automation Solution if they are no longer needed.	Having this capability means that the service provider has an identifiable process for producing a report that confirms that accounts that were created to support its activities have been removed once those activities are complete. The intent is to ensure that the Automation Solution does not contain or retain service provider accounts unless they are needed. See SP.08.02 BR for the requirement to log security-related events, which includes the removal of these accounts.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.09.05	BR	Account management	Passwords	Composition	No	The service provider shall have the capability to ensure that password policies can be set to achieve a minimum complexity commonly accepted by both the security and industrial automation communities. NOTE At the time of this writing, minimal password complexity is: 1) at least eight characters in length and 2) a combination of at least three of the following four character sets: lowercase, uppercase, numeric digit, and special characters (e.g.% and #).	The capability specified by this BR is used to ensure that the service provider can support a broad range of asset owner password complexity policies. Using complex passwords makes password discovery more difficult. Having this capability means that the service provider has an identifiable process for ensuring that the Automation Solution supports complex passwords. The password complexity used within a specific Automation Solution is beyond the scope of this requirement. See IEC 62443-3-3 for related security requirements for systems used in Automation Solutions, and IEC 62443-3-2 for the use of risk assessments to aid in the determination of the level of password complexity to be used for a specific Automation Solution. Also see IEC 62443-2-1 for password policy requirements for asset owners.
SP.09.06	BR	Account management	Passwords	Expiration	No	The service provider shall have the capability to ensure that passwords for local and system-wide (e.g. domain) user accounts are configured to automatically expire after they have been in use for a period of time specified by the asset owner.	The capabilities specified by this BR and its RE are used to ensure that passwords can be changed periodically. Passwords that remain unchanged increase the risk that they will be disclosed/discovered and used to gain unauthorized access to the system. In addition, changing passwords periodically limits the length of time an attacker has to discover a password. Having this capability means that the service provider has an identifiable process for ensuring that passwords can be configured to automatically expire after they have been in use for an asset owner specified number of days. When and how often the service provider verifies that the password expiration period is Automation Solution specific, but verification is typically done as part of the handover process and at after or during each maintenance cycle. The asset owner's security policy should set the expiration period based on a risk assessment and this value should be periodically be reviewed. See IEC 62443-3-2 for more information on risk assessment, IEC 62443-3-3 for related requirements for control systems product capabilities, and IEC 62443-2-1 for related requirements for asset owners. NOTE IEC 62443-2-1 does not explicitly mention lifetime requirements for passwords, but does address more general password policies.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.09.06	RE(1)	Account management	Passwords	Expiration	No	The service provider shall have the capability to ensure that password policies are set to prompt users to change passwords *N* days before they expire, where *N* is specified by the asset owner. This requirement does not apply to passwords that are not set to expire.	Having this capability means that the service provider has an identifiable process for ensuring that users are notified that their passwords are expiring so they have time to change them.
SP.09.07	BR	Account management	Passwords	Change	No	The service provider shall have the capability to ensure that default passwords are changed as required by the asset owner.	The capability specified by this BR is defined to prevent default passwords that have become well-known from being used in any Automation Solution. Having this capability means that the service provider has an identifiable process for ensuring that default passwords are changed according to asset owner requirements. Typically, this will be on installation, re-installation, and reset/recovery.
SP.09.08	BR	Account management	Passwords	Reuse	No	The service provider shall have the capability to ensure that password policies are set to prevent users from reusing their last *N* passwords, where *N* is specified by the asset owner.	The capabilities specified by this BR and the its RE are defined to prevent users from changing their passwords and then immediately changing them back, which would effectively mean that their passwords were not changed. Having this capability means that the service provider has an identifiable process for verifying that the password reuse policy is set to the number specified by the asset owner.
SP.09.08	RE(1)	Account management	Passwords	Change	No	The service provider shall have the capability to ensure that password policies are set to prevent users from changing their passwords more frequently than once every N days, where N is specified by the asset owner.	Having this capability means that the service provider has an identifiable process for configuring password policies to prevent users from changing password continuously to get back to a favorite password. The period of *N* days means that once a password has been changed, the user cannot change it again for *N* days.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.09.09	BR	Account management	Passwords	Shared	No	The service provider shall have the capability to ensure that accounts whose passwords have been approved by the asset owner to be shared with the service provider are securely documented and maintained.	The capabilities specified by this BR and its RE are used to ensure that the use of shared passwords is managed. Without management of shared passwords, the asset owner may not be aware of or lose track of who has access to the Automation Solution. Having this capability means that the service provider has an identifiable process for documenting the list of accounts for which passwords have been divulged to it by the asset owner and protecting that list from unauthorized disclosure and modification. The service provider is accountable and responsible for maintaining a log of who has been given passwords for these accounts, including its subcontractors, consultants, and representatives.
SP.09.09	RE(1)	Account management	Passwords	Shared	No	The service provider shall have the capability to report to the asset owner passwords that were 1) shared and no longer need to be shared, 2) knowingly divulged, or 3) knowingly compromised, and to support the asset owner in changing passwords as necessary.	Having this capability means that the service provider has an identifiable process for keeping track of passwords (including passwords for auto-login accounts) that were shared with the service provider or that the service provider knows were compromised or otherwise divulged to others, and for reporting them to the asset owner so they can be changed. For example, the service provider will need to report passwords shared within the service provider organization to the asset owner once they are no longer needed by the service provider. To change these passwords, the asset owner may require the service provider's support. Similarly, if service provider personnel share passwords with others, the service provider will need to report these accounts/passwords to the asset owner when they no longer need to be shared. Sharing of passwords often occurs during testing, commissioning, troubleshooting, and maintenance. In addition, any time the service provider suspects that a password has been compromised, it should notify the account owner and request that the password be changed.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.10.01	BR	Malware protection	Manual process	Malware protection mechanism	No	The service provider shall have the capability to provide the asset owner with documented instructions for the proper installation, configuration and update of malware protection mechanisms that are tested and verified for the Automation Solution.	The capability specified by this BR is used to ensure that the asset owner has the documentation necessary to use the anti-malware mechanisms that are compatible with the Automation Solution. Having this capability means that the service provider has an identifiable process for providing the documentation for commonly accepted malware protection software (e.g. anti-virus, whitelisting) that operates as intended on Automation Solution hardware platforms (e.g. workstations) for which the service provider is responsible. If the control system supplier does not test and recommend an anti-malware product, then the service provider needs to be able to have these capabilities.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.10.02	BR	Malware protection	Security tools and software	Installation	No	The service provider shall have the capability to ensure that: 1) malware protection mechanisms have been correctly installed/updated and properly configured in accordance with the service provider's approved procedures, 2) malware definition files are installed within the time period agreed to with the asset owner, 3) malware configurations are maintained and kept current.	The capabilities specified by this BR and its RE are used to ensure that the Automation Solution is protected against malware. Having this capability means that the service provider has an identifiable process for applying and managing anti-malware software for Automation Solution platforms for which the service provider is responsible. This includes installing and updating anti-malware software, keeping its malware definition files current, and maintaining its operational configuration settings. The intent is to have anti-malware software with its latest definition files, operational configuration, and software updates running on all relevant hardware platforms in the Automation Solution. Having this capability also means that the service provider has an identifiable process for coming to agreement with the asset owner on the time period between the release of the malware definition files and their installation. EXAMPLE 1 If anti-virus software is used, installation of anti-virus definition files is performed within the agreed-to time period. EXAMPLE 2 If whitelisting software is used, whitelisting configurations are kept current. EXAMPLE 3: Keeping a log of the installation and configuration activities, including updates to software and malware definition files, is a way of demonstrating this capability.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.10.02	RE(1)	Malware protection	Security tools and software	Installation	No	The service provider shall create and maintain the documentation that describes the use of malware protection mechanisms in the Automation Solution for which the service provider is responsible. This documentation shall include for each component used in the Automation Solution: 1) the installation state of malware protection mechanisms or a statement that it is not technically possible to install malware protection mechanisms on the component, 2) the current configuration settings of the installed malware protection mechanism, 3) the current status of malware definition files approved for installation on the component, 4) the use of other mitigating features and functions used to reduce the risk of infection and/or mitigate the effect of infections (e.g. isolating infections, reporting infections).	Having this capability means that the service provider has an identifiable process for documenting the anti-malware software status for each hardware platform in the Automation Solution, whether or not anti-malware software is installed on the component. All platforms are required to have anti-malware software installed, except where it is not technically feasible (e.g. no anti-malware software exists).
SP.10.03	BR	Malware protection	Security tools and software	Detection	No	The service provider shall have the capability to verify that malware, other than zero-day malware, can be detected and properly handled by the installed malware protection mechanisms.	The capability specified by this BR is used to verify that anti-malware mechanisms work as intended. Having this capability means that the service provider has an identifiable process for verifying that an infected file can be detected and subsequently quarantined/deleted by the anti-malware product. The only exception is a zero-day infection, which is an infraction for which there is no malware definition file available. This is generally the case when the malware has not been previously seen or detected.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.10.04	BR	Malware protection	Manual process	Malware definition files	Yes	The service provider shall have the capability to provide to the asset owner documentation that describes: 1) how malware definition files for the Automation Solution are evaluated and approved, 2) reporting the status of malware definition files to the asset owner within *N* days after release of the files by the manufacturer, where *N* has been agreed to by the service provider and asset owner. This status includes the applicability (e.g. component and version) and approval state (e.g. approved, installed, disapproved, etc.) for each malware definition file.	The capability specified by this BR is used to ensure that service provider has a process for verifying that new malware definition files are compatible with the Automation Solution and that they are available to the Automation Solution in a timely manner. Having this capability means that the service provider has an identifiable process for approving malware definition files and informing the asset owner of the results within a mutually agreed to time period after their release by the anti-malware software manufacturer. This does not require installation within this time-period, it requires only that files are approved for installation within the time period. Approval means that the service provider has evaluated the files for conflicts with their system. Those that conflict with the operation of the system are not approved.
SP.10.05	BR	Malware protection	Devices – All	Sanitizing	No	The service provider shall have the capability to ensure that all devices, including workstations, supplied to the Automation Solution by the service provider are free of known malware prior to use in the Automation Solution.	The capability specified by this BR is used to ensure that devices with detectable infections are not installed in the Automation Solution. The term “known malware” is used to indicate malware that has been previously discovered and for which malware definition files have been developed and are available. Having this capability means that the service provider has an identifiable process for verifying/ensuring that malware is not present in equipment provided by it to the Automation Solution. Verification can include checking the equipment for malware, installing software to the equipment at the site from malware-free media (see SP.10.05 RE(2)), and/or ensuring the supply chain provides malware free equipment (e.g. the control system vendor performs malware scans prior to delivery). See ISO 27036 for more information on supply chain security.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.10.05	RE(1)	Malware protection	Portable media	Usage	No	The service provider shall have the capability to ensure that for portable media that it uses for system testing, commissioning, and/or maintenance, it uses this portable media for this purpose only.	The capability specified by this RE is used to ensure that portable media are not used outside the Automation Solution to reduce the possibility of them becoming infected with malware. Having this capability means that the service provider has an identifiable process for ensuring that it does not use portable media that it uses in support of the Automation Solution (that has the possibility of infecting the Automation Solution with malware) in other places where it could be infected. For example, if a USB memory device has diagnostics tools or data on it, then this device should not be connected to any workstation or server that is not part of the Automation Solution.
SP.10.05	RE(2)	Malware protection	Portable media	Sanitizing	No	The service provider shall have the capability to ensure that all portable media used in or connected to the Automation Solution by the service provider is free of known malware prior to use in the Automation Solution.	The capability specified by this RE is used to ensure that portable media with detectable infections are not used in the Automation Solution. The term “known malware” is used to indicate malware that has been previously discovered and for which malware definition files have been developed and are available. Having this capability means that the service provider has an identifiable process for procedures to prevent infected portable devices from infecting the Automation Solution. Types of portable media include but are not limited to: installation media, CD / DVD/ Blu-ray Media, USB memory devices, smart phones, flash memory, solid state disks, hard drives, and portable computers. See SP.07.XX for requirements associated with remote connection to the Automation Solution.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.11.01	BR	Patch management	Manual process	Patch qualification	Yes	The service provider shall have the capability to provide documentation to the asset owner that describes how security patches for Automation Solution software for which it is responsible are evaluated and approved. NOTE 1 In this standard, firmware upgrades are regarded as software patches. NOTE 2 In this standard, patch installation refers to installation of patches to the Automation Solution.	The capability specified by this BR is used to ensure that service provider has a documented process that can be reviewed by the asset owner for verifying that new software security patches are compatible with the Automation Solution (see SP.10.04 BR). In many cases, the service provider will use documentation from the control system product supplier and modify it for the Automation Solution if necessary. Having this capability means that the service provider has an identifiable process for providing a document to the asset owner that describes its policies for determining which security patches apply to the Automation Solution, and how they are tested and approved. This includes security patches for the control system and component software, operating system software, and 3rd party software applications integrated into or with the Automation Solution, the control system, and components. IEC TR 62443-2-3 describes patch management and outlines a set of associated responsibilities for the control system supplier and the asset owner. SP 11.XX defines patch management capabilities for the service provider in support of the IEC TR 62443-2-3 asset owner patch management responsibilities.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.11.01	RE(1)	Patch management	Manual process	Patch qualification	No	The service provider shall have the capability to review, as a result of changes in security risks, how it evaluates and approves security patches for Automation Solution software for which it is responsible.	The capability specified by this RE is used to ensure that service provider is able to update its patch evaluation process in response to changes in the cyber-security threat landscape. (e.g. new threats may require a more rapid response). Typically, this is demonstrated as part of its incident handling capabilities or as a separate process for periodically reviewing its patch evaluation process. Having this capability means that the service provider has an identifiable process for reviewing its process for evaluating and approving security patches. These reviews are required to be performed to be able to update this process to address changes in the risk environment. This review needs to be performed periodically or explicitly in response to significant changes in the risk environment. Significant changes are those that are recognized to have a potential impact on the process. Changes to the risk environment generally includes new threats and vulnerabilities as well as the development of new security technologies.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.11.02	BR	Patch management	Patch list	Patch qualification	Yes	The service provider shall have the capability to make documentation available to the asset owner that describes security patches/updates. The description of each patch shall be available to the asset owner within an agreed time frame after the release of a patch by its manufacturer, and shall include: 1) security patches that are applicable to components of the Automation Solution for which the service provider is responsible, 2) the approval status/lifecycle state (see IEC TR 62443-2-3) of each; i.e., approved, not approved, not applicable, in test, 3) a warning if the application of an approved patch requires or causes a re-start of the system, 4) the reason for those that are not approved or not applicable, 5) a plan for the remediation for those that are applicable but not approved.	The capabilities specified by this BR and its REs are used by the asset owner to access descriptions of security patches that are relevant to the Automation Solution from the service provider and to have the service provider recommend how to mitigate vulnerabilities for patches the asset owner choose not to install. Having this capability means that the service provider has an identifiable process for evaluating and approving security patches as documented by the capability defined in SP.11.01 BR, and for informing the asset owner of the results within *N* number of days after the release of the patch by its manufacturer, where *N* is agreed to by the service provider and the asset owner. The service provider may use software libraries that are enhanced or otherwise different than those provided by their manufacturer(s). In this case, the service provider may need to alter a software patch package. This type of issue needs to be addressed as part of this requirement.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.11.02	RE(1)	Patch management	Patch list	Patch qualification	No	The service provider shall have the capability to make available to the asset owner, through an interface commonly accepted by the industrial and security communities, a patch list that identifies: 1) approved security patches applicable to Automation Solution software for which the service provider is responsible (e.g. control system and component software, operating system software, and 3rd party software applications), 2) which of the applicable security patches have been approved for use in the Automation Solution, 3) the version numbers of the software to which the approved patches apply. This list shall be available to the asset owner within an agreed timeframe after the release of a patch by the manufacturer.	Having this capability means that the service provider has an identifiable process for describing to the asset owner how to electronically retrieve a list that describes the approved security patches that are applicable to components for which the service provider is responsible (see SP.11.02 BR). This list is to be provided through a commonly accepted interface to allow the asset owner to know which patches it needs to download from the manufacturer or obtain otherwise obtain them. This list may be retrieved through this interface from the control system product supplier, from the service provider, or from another agent identified by the service provider. NOTE Approved is meant to imply that the patches have been tested and validated by the service provider against a known configuration and no issues were found.
SP.11.02	RE(2)	Patch management	Patch list	Approval	No	The service provider shall have the capability to: 1) recommend a mitigation plan when requested by the asset owner for security patches that were applicable and approved by the service provider, but that were not approved by the asset owner, for example, because they could impact operations or performance (see SP 11.05 BR), 2) implement the mitigation plan after approval by the asset owner.	Having this capability means that the service provider has an identifiable process for developing and implementing an approach to mitigate the impact of not being permitted to install a security patch that could negatively impact the Automation Solution. This approach may include compensating mechanisms or other means to reduce the vulnerabilities addressed by the security patch. Alternative approaches are subject to asset owner approval.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.11.03	BR	Patch management	Security patch	Delivery	No	The service provider's management of patches shall provide for: 1) patches to be obtained by the asset owner directly from the patch's manufacturer, and/or 2) redistribution of patches by the service provider only if approved by the asset owner and permitted by the patch manufacturer.	The capability specified by this BR is used to ensure that patches are obtained through an authorized channel (from an appropriate source) to reduce the possibility that they could be invalid/infected. Having this capability means that the service provider's patch delivery policy supports having the asset owner obtain the patch directly from the patch manufacturer, or from the service provider at the request of the asset owner, and then only if the licensing agreements with the patch manufacturer permit this. If the patches are to be delivered by the service provider, then the service provider and the asset owner will have to jointly decide how this will occur (e.g. DVD, secure connection).
SP.11.04	BR	Patch management	Security patch	Installation	Yes	The service provider shall have the capability to provide documentation to the asset owner that describes how to perform patching both manually and via a patch management server and how to obtain patching status reports. 1) When using a patch management server, documentation shall be provided to show how to use the server to install patches. 2) For manual patching using portable media, documentation shall be provided that describes how to install patches from the media.	The capability specified by this BR is used to ensure that the asset owner knows how to install security patches for the Automation Solution. Having this capability means that the service provider is able to provide instructions to the asset owner that describes how to install patches from portable media (e.g. CDs, DVDs, USB memory devices) and from a patch management server.
SP.11.05	BR	Patch management	Security patch	Approval	No	The service provider shall have the capability ensure that it obtains approval from the asset owner for installing each and every security patch.	The capability specified by this BR is used to ensure that the service provider installs patches if and only if the asset owner wants them to be installed. Having this capability means that the service provider has a policy that requires it to obtain approval from the asset owner to install patches.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.11.06	BR	Patch management	Security patch	Installation	No	The service provider shall have the capability to ensure that if the asset owner requests the service provider to install security software patches (including firmware upgrades), the service provider installs them at a time specified by the asset owner.	The capability specified by this BR is used to ensure that the service provider installs patches only when the asset owner wants them to be installed, for example, to prevent process upset if a device has to reboot after installation. Having this capability means that the service provider has an identifiable process for installing approved patches only at a time specified by the asset owner.
SP.11.06	RE(1)	Patch management	Security patch	Installation	No	The service provider shall have the capability to ensure that the security hardening level of the Automation Solution is retained after patch installation, e.g. by reinstalling software or changing system configuration settings.	The capability specified by this RE is used to ensure that patch installation does not "undo" or otherwise degrade the hardening of the Automation Solution. Having this capability means that the service provider has an identifiable process for ensuring that it has a process for restoring the hardening state of the Automation Solution if patch installation causes it to degrade. This capability is independent of who installs the patches. It is not uncommon for the installation of patches and system updates to require or automatically restore configuration settings that remove or degrade system hardening, such as the installation of a Service Pack from Microsoft. Therefore, the service provider has to have a process that determines if this has happened, and if it has to restore the hardening.
SP.11.06	RE(2)	Patch management	Security patch	Installation	No	The service provider shall have the capability to ensure that, for devices that support installation of software/firmware over the network, the update process ensures the authenticity and integrity of the device software/firmware.	The capability specified by this RE is used to ensure that patches installed over the network are authentic and have not been corrupted prior to or during the patching process. Having this capability means that the service provider has an identifiable process for securely updating the software/firmware in devices. This includes allowing only authorized users to perform updates, and also ensuring that update images sent to devices are authentic (not counterfeit or corrupted) and are protected against corruption during the update process. Patching may expose software images to the network. See SP.03.10 BR and its REs for the safeguarding of sensitive data. See IEC 62443-3-3 and IEC 62443-4-2 for requirements related to authentication, authorization, integrity, and confidentiality.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.11.06	RE(3)	Patch management	Security patch	Installation	No	The service provider shall have the capability to determine the installation status of all security patches applicable to the Automation Solution for which the service provider is responsible.	Having this capability means that the service provider has an identifiable process for tracking whether patches approved for the Automation Solution have been installed for the purpose of determining which patches are missing (not installed). This capability may be provided with either manual procedures or automated tools.
SP.12.01	BR	Backup/Restore	Manual process	Technical description	Yes	The service provider shall have the capability to provide documentation for recommended backup procedures for the Automation Solution that includes, but is not limited to the following: 1) Instructions on how to make a full backup of the Automation Solution, and partial backups if applicable, using at least one of the following methods a) proprietary backup architecture on removable media, b) single system backup architecture on removable media, c) distributed back-up architecture in which each backup system backs up a subset of the service provider's Automation Solutions at the asset owner's site, or d) centralized back-up architecture using one backup system for all fo the service provider's Automation Solutions at the asset owner's site.	The capability specified by this BR ensures that the asset owner knows how to use the backup capabilities provided by the service provider for the Automation Solution. Having this capability means that the service provider has an identifiable process for preparing a document specific to the Automation Solution that defines how to backup the Automation Solution, which data to backup to support full and partial backups, and how it recommends off-site storage to be handled. This documentation should recognize that: 1) The backup image is regarded as sensitive (see SP.03.10 BR and its REs for the safeguarding of sensitive data) and may therefore be a target for security compromise. 2) The backup may be needed to recover from security incidents (e.g. a workstation becomes corrupted). 3) The asset owner may have a backup strategy that is generally dependent of business requirements. 4) The asset owner's backup strategy may include topics related to backup frequency, partial backups, when backups should be performed (e.g. prior to engineering changes), and recovery from infection that may influence the contents of the service provider documentation. 5) Backups should be allowed to complete before changes are made that could interrupt the backup or that could cause inconsistencies in the backup data. Examples of such changes include engineering changes and patch installation.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
						2) Provisions to back-up the following types of data a) operation system files and cryptographic data (e.g. keying material), b) applications(including middleware, such as tunneling software), c) configuration data, database files, d) log files, electronic log book, e) unconventional file types including, but not limited to network equipment settings, control system controller settings (tuning parameters, set points, alarm levels), f) field instrumentation parameters, and g) directory information h) other files identified by the service provider that are required to create a complete backup of the Automation Solution, 3) Recommendations for offsite storage of backup media, 4) Provisions to ensure changes to the Automation Solution that could affect the integrity of a backup are not made while a backup is in progress NOTE Examples of partial restores include operating system, application software, databases, and configuration files.	

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.12.02	BR	Backup/Restore	Restore	Technical description	Yes	The service provider shall have the capability to provide documented instructions to the asset owner for restoring the Automation Solution or its components to normal operation.	The capability specified by this BR ensures that the asset owner knows how to use the restore capabilities provided by the service provider for the Automation Solution. Having this capability means that the service provider has an identifiable process for preparing or providing documentation that describes how to restore the Automation Solution or its components (i.e. a partial restore) from backup data. The documentation should include instructions for handling abnormal scenarios, such as how to restore an Automation Solution whose architecture may have changed since the backup was made. In these cases, the restore may not be complete and the asset owner should be made aware of conditions such as these. This requirement applies to both operational Automation Solutions and simulations.
SP.12.03	BR	Backup/Restore	Portable media	Technical description	Yes	The service provider shall have the capability to provide documentation to the asset owner that describes how to control and securely manage removable backup media.	The capability specified by this BR ensures that the asset owner knows how to securely handle the backup media for the Automation Solution. Having this capability means that the service provider has an identifiable process for preparing a document specific to the Automation Solution that describes handling of backup data to adequately protect it that is consistent with, or extensions of, asset owner policies and procedures. Backup data can be a target for compromise, for example, to prevent proper restoration or to gain access to confidential data.
SP.12.04	BR	Backup/Restore	Backup	Verification	Yes	The service provider shall have the capability to provide documentation to the asset owner that describes how to verify successful system backup.	The capability specified by this BR ensures that the asset owner knows how to verify the backup of the Automation Solution. Having this capability means that the service provider has an identifiable process for preparing (or providing) a document that describes how to verify the success of a backup.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.12.05	BR	Backup/Restore	Restore	Verification	No	The service provider shall have the capability to verify that: 1) it is possible to perform a complete back-up of the Automation Solution, and 2) it is possible to restore a fully functioning Automation Solution from this back-up.	The capability specified by this BR ensures that the backup and restore capabilities for the Automation Solution work as intended. Having this capability means that the service provider has an identifiable process for demonstrating or otherwise verifying that a backup can be performed successfully and that the Automation Solution can be restored from this backup. This process should be flexible to allow the asset owner to request only a partial backup/restore to gain confidence that the backup capability can be used successfully. If the backup includes the backup of data bases, then having this capability also means that the service provider has an identifiable process for demonstrating or otherwise verifying that automatic rollback is stopped/disabled prior to starting the backup. Automatic rollback can cause inconsistencies in the data base should it occur while the data base is being backed up.
SP.12.06	BR	Backup/Restore	Backup	Perform	No	The service provider shall have the capability to perform a backup of the Automation Solution in accordance with the asset owner's backup schedules and data restore and disaster recovery objectives.	The capability specified by this BR ensures that, when backing up the Automation Solution, the service provider follows the guidance/policies of the asset owner. Having this capability means that the service provider has an identifiable process for adhering to the asset owner's backup/restore strategies and objectives, including backup schedules and disaster recovery plans (see SP.12.09 BR). The intent of this requirement is to ensure that the service provider is prepared to integrate its backup/restore activities with the asset owner's backup requirements.
SP.12.07	BR	Backup/Restore	Backup	Robustness	No	The service provider shall have the capability to ensure that the Automation Solution is able to continue normal operation during a backup.	The capability specified by this BR ensures that operation of the Automation Solution (e.g. control of the process) is not impacted by the backup process. Having this capability means that the service provider has an identifiable process for ensuring that the backup operations do not interfere with normal operations of the Automation Solution. For related system capability requirements, see IEC 62443-3-3.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.12.08	BR	Backup/Restore	Manual process	Logging	Yes	The service provider shall have the capability to provide documentation to the asset owner that describes how to generate and maintain audit logs of all backup and restore activities.	The capability specified by this BR ensures that the asset owner knows how to manage audit logs for the backup and restore operations. These audit logs provide evidence of backup/restore activities such as when they occurred, who performed them, and their status. Having this capability means that the service provider has an identifiable process for preparing or providing documentation that describes how to configure the Automation Solution to write backup and restore actions to an audit log.
SP.12.09	BR	Backup/Restore	Manual process	Disaster recovery	Yes	The service provider shall have the capability to document a recommended disaster recovery plan that includes, but is not limited to the following: 1) Description of various disaster scenarios and their impact on the Automation Solution, 2) Step-by-step instructions for restoring, restarting, failed components and integrating them into the Automation Solution, 3) Minimum architecture requirement for restoring the entire Automation Solution.	The capability specified by this BR ensures that not only is there is a plan for recovering from a disaster, but also that the details of how a disaster could occur (e.g. including cyber-security threats), and how to recover from the disaster. Having this capability means that the service provider has an identifiable process for preparing a document specific to the Automation Solution that defines how to manage a major crisis based on a cyber-security scenario for restoring the Automation Solution and its components. The back-up and the means of restoration cannot be compromised by loss of the Automation Solution components or the entire Automation Solution. The means of restoration may include equipment, such as test bench or off-line development tools.

Bibliography

NOTE This bibliography includes references to sources used in the creation of this standard as well as references to sources that may aid the reader in developing a greater understanding of cybersecurity as a whole and of the process of developing a cybersecurity management system. Not all references in this bibliography are referred to throughout the text of this standard.

IETF/RFC 1510, The Kerberos Network Authentication Service (V5)

CMMI® for Services, Version 1.3, November 2010, (CMU/SEI-2010-TR-034, ESC-TR-2010-034)

ISO/IEC 27036-3, *Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security*

ISO/IEC 30111, *Information technology – Security techniques – Vulnerability handling processes*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*

IEC 62264-1:2013: *Enterprise-control system integration – Part 1: Models and terminology*

IEC 62351-8:2011, *Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control*

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

IEC/TR 62443-1-2, *Industrial communication networks – Network and system security – Part 1-2: Master glossary of terms and abbreviations*[1]

IEC/TR 62443-1-3, *Industrial communication networks – Network and system security – Part 1-3: System security compliance metrics*[2]

IEC 62443-2-1:2010 *Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program*

IEC/TR 62443-2-3, *Industrial communication networks – Network and system security Part 2-3: Patch management in the IACS environment*[3]

IEC 62443-3-2, *Industrial communication networks – Network and system security – Part 3-2: Security assurance levels for zones and conduits*[4]

[1] Under consideration.

[2] Under preparation.

[3] Under preparation.

IEC 62443-3-3:2013, *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*

IEC 62443-4-1, *Industrial communication networks – Network and system security – Part 4-1: Product development requirements*[5]

IEC 62443-4-2, *Industrial communication networks – Network and system security – Part 4-2: Technical security requirements for IACS components*[6]

IEC TR 62443-4-2-1, *Industrial communication networks – Network and system security – Part 4-2-1: WIB Profiles*[7]

____

[4] Under preparation.

[5] Under consideration.

[6] Under consideration.

[7] Under consideration.

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch