IEC 62443-2-4

Edition 1.0 2015-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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

IEC 62443-2-4:2015-06(en-fr)

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 It also gives information on projects, replaced and withdrawn publications.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 more than 30 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
More than 60 000 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.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Catalogue IEC - webstore.iec.ch/catalogue
Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - www.iec.ch/searchpub
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,…). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org
Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
Plus de 60 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

IEC 62443-2-4

Edition 1.0 2015-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 25.040.40; 35.040; 35.100

ISBN 978-2-8322-2767-1

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

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

FOREWORD

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

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

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

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

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

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

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

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

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

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

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

INTRODUCTION

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

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

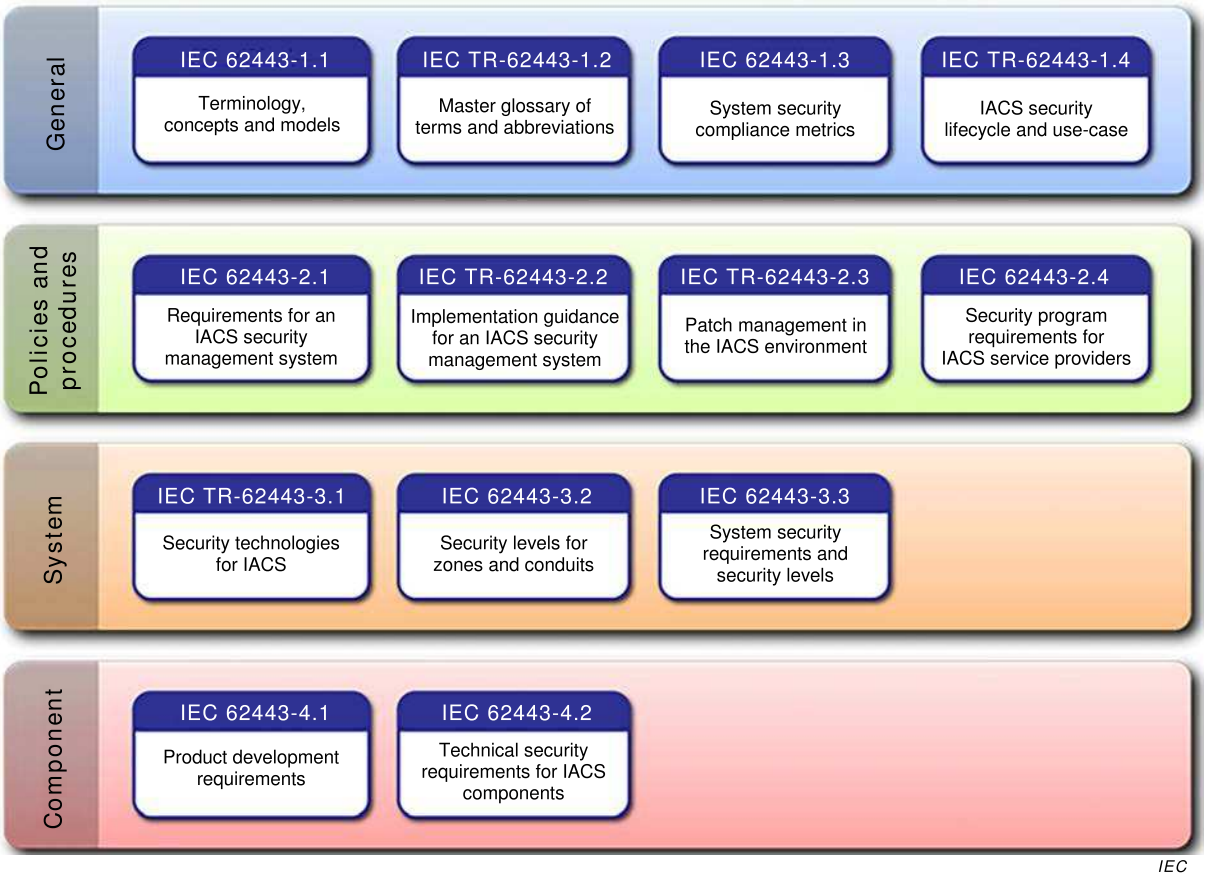

Figure 1 – Parts of the IEC 62443 Series

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

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

1 Scope

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

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

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

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

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

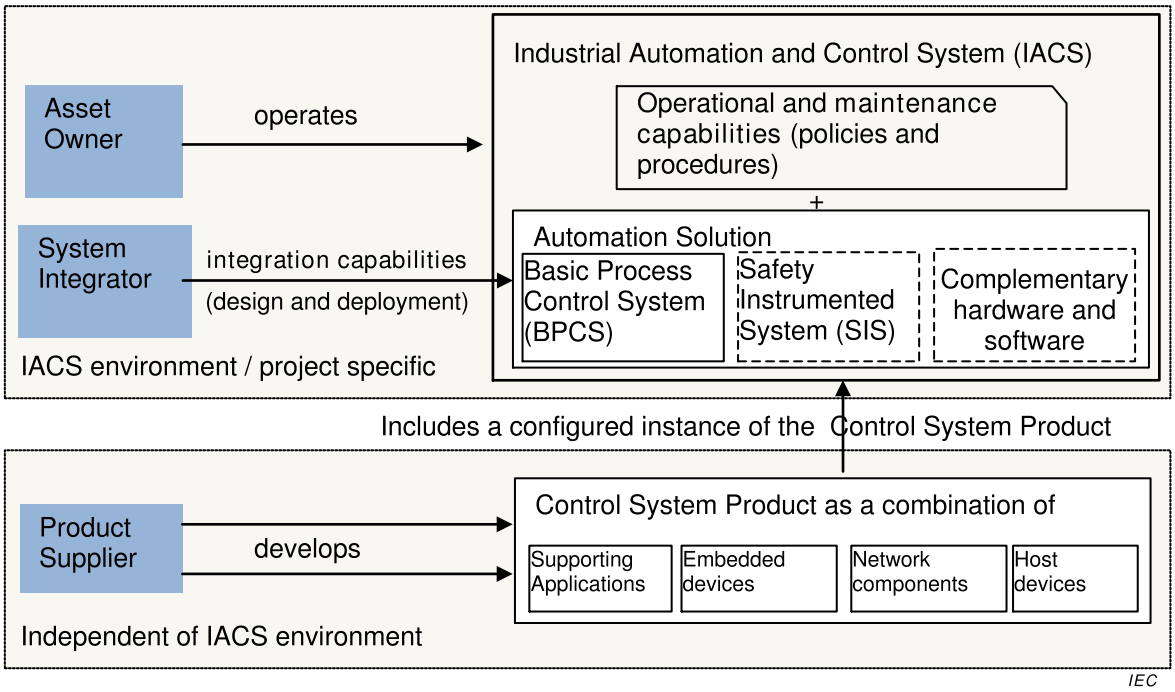

Figure 2 – Scope of service provider capabilities

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

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

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

NOTE 5 Automation Solutions typically have a single control system (product), but they are not restricted to do so. In general, the Automation Solution is the set of hardware and software, independent of product packaging, that is used to control a physical process (e.g. continuous or manufacturing) as defined by the asset owner.

2 Normative references

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

“None”

3 Terms, definitions, abbreviated terms and acronyms

3.1 Terms and definitions

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

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

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

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

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

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

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

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

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

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

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

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

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.

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.

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.

It is anticipated that asset owners will select existing profiles to specify the requirements that they need for 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 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.

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. 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 organization of the requirements. Table 3 provides a list of the functional areas.

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

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.

The phrase “commonly accepted by both the security and industrial automation communities” is used in these requirement descriptions to prevent requirements for specific 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.

5.5.8 Rationale

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.
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 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. 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.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
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 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. 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 the capability to assign security leads to Automation Solutions who have demonstrated expertise in IACS cybersecurity.	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 an identifiable process for staffing each Automation Solution with personnel who are sufficiently qualified to lead cyber-security related activities. 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" is used to indicate that the security leads assigned to the Automation Solution have evidence that shows their relevant experiences.
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 Level 2 from 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 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 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 between the SIS and the BPCS (e.g. configuration downloads, status monitoring, logging) be separated 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 critical communications. Having this capability means that the service provider is able to logically or physically isolate functional safety communication from other Automation Solution traffic for SIL 1 and above (see IEC 61508). Having this capability means 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. 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. 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. Having this capability means that the service provider has an identifiable process for ensuring that the SIS cannot be connected, physically or logically, to Level 3 or above. Applications above Level 2 are not allowed to connect directly to the SIS.
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).	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. Having this capability means that the service provider has an identifiable process for ensuring that there are no safety-critical communications (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 from being compromised by traffic originating from sources outside the SIS.

Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
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 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 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).
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.	The capability specified by this RE is defined to be able to prevent SIS engineering workstations from being exploited via remote access connections. Having this capability means that the service provider has an identifiable process for ensuring that SIS engineering workstations either (1) do not have remote access installed or (2) have it disabled. 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 is: 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: 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 the Automation Solution's SIS EWS is restricted to performing SIS functions.	The capability specified by this BR is used to reduce the possibility that the SIS EWS will contain software 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.
SP.05.08	BR	SIS	Devices – Wireless	Connectivity	No	The service provider shall have the capability to verify that wireless devices are not allowed as an integral part of SIS safety functions.	The capability specified by this BR is used to prevent wireless attacks against the SIS since wireless devices are not bounded by physical security perimeters nor by physical implementation. 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 that wireless device communications are not used within the SIS.
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. While locked, 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 ensure that the Automation Solution provides a 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	The service provider shall have the capability to ensure that the Automation Solution is able 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 denial of service during event storms. The characteristics of event storms (e.g. number of events/second) is 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. 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.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 are 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 passwords that have been divulged to it by the asset owner. The service provider is accountable and responsible for maintaining a log of the usage of each account by its personnel, 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.
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 anti-malware software for Automation Solution hardware for which the service provider is responsible. The intent is to have anti-malware software with its latest data, 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.

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. 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 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. 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: 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 not corrupted 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. 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.

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

SÉCURITÉ DES AUTOMATISMES INDUSTRIELS ET DES SYSTÈMES DE COMMANDE –

Partie 2-4: Exigences de programme de sécurité pour les fournisseurs de service IACS

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 62443-2-4 a été établie par le comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels.

Le texte de cette norme est issu des documents suivants:

CDV	Rapport de vote
65/545CDV	65/561A/RVC

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette publication a été rédigée selon les Directives ISO/IEC, Partie 2.

Une liste de toutes les parties de la série IEC 62443, publiées sous le titre général *Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes,* peut être consultée sur le site web de l'IEC.

Les futures normes de cette série porteront dorénavant le nouveau titre général cité ci-dessus. Le titre des normes existant déjà dans cette série sera mis à jour lors de la prochaine édition.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

La présente norme est la partie de la série IEC 62443 qui contient les exigences de sécurité pour les fournisseurs de service d'intégration et de maintenance pour les systèmes d'automatisation et de commande industrielles (IACS). Elle a été élaborée par la Comité d'études 65 de l'IEC en collaboration avec l'International Instrumentation Users Association (appelée WIB, qui est son nom d'origine et désormais obsolète en néerlandais) et les membres du comité ISA 99.

La Figure 1 représente les relations entre les différentes parties de l'IEC 62443 en cours d'élaboration. Celles qui sont citées en référence de manière normative sont incluses dans la liste des références normatives de l'Article 2, et celles qui sont citées en référence à titre d'information ou qui sont en cours d'élaboration sont énumérées dans la Bibliographie.

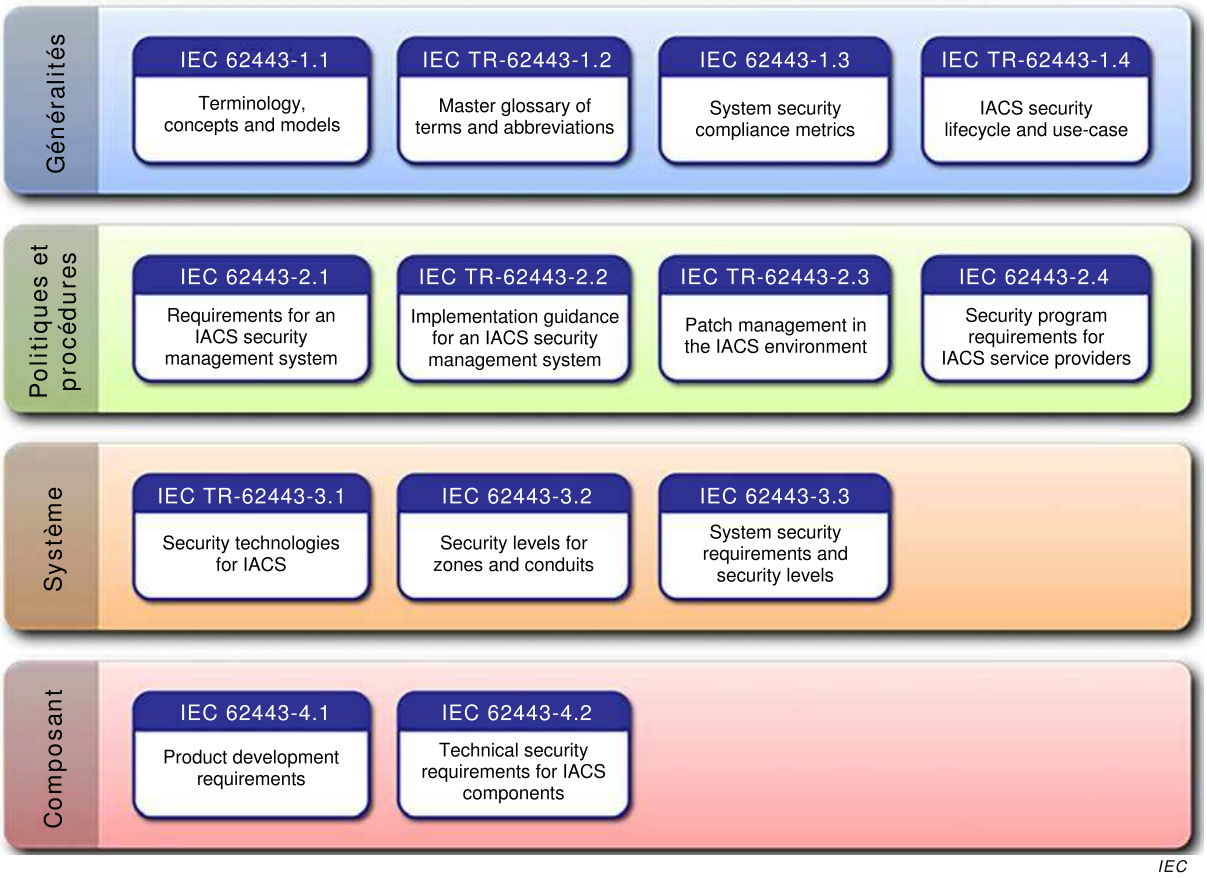

Figure 1 – Parties de la série IEC 62443

SÉCURITÉ DES AUTOMATISMES INDUSTRIELS ET DES SYSTÈMES DE COMMANDE –

Partie 2-4: Exigences de programme de sécurité pour les fournisseurs de service IACS

1 Domaine d'application

La présente partie de l'IEC 62443-2-4 spécifie les exigences de capacités de sécurité pour les fournisseurs de service IACS qu'ils peuvent proposer au propriétaire d'actif pendant les activités d'intégration et de maintenance d'une Solution d'Automatisation.

NOTE 1 Dans la présente partie de l'IEC 62443, le terme ''Solution d'Automatisation'' est utilisé comme un nom propre (et par conséquent écrit en majuscule) pour éviter toute confusion avec d'autres usages de ce terme.

De manière collective, les capacités de sécurité offertes par un fournisseur de service IACS sont appelées Programme de sécurité. Une spécification associée, l'IEC 62443-2-1 décrit les exigences pour le Système de gestion de sécurité du propriétaire d'actif.

NOTE 2 En général, ces capacités de sécurité sont liées à la politique, la procédure, la pratique et au personnel.

La Figure 2 représente la relation entre les capacités d'intégration et de maintenance et l'IACS ainsi que le produit de système de commande intégré à la Solution d'Automatisation. Certaines de ces mesures de sécurité de référence en matière de capacités définies dans l'IEC 62443-3-3 que le fournisseur de service doit assurer sont prises en charge dans la Solution d'Automatisation (soit incluses dans le produit de système de commande soit séparément ajoutées à la Solution d'Automatisation).

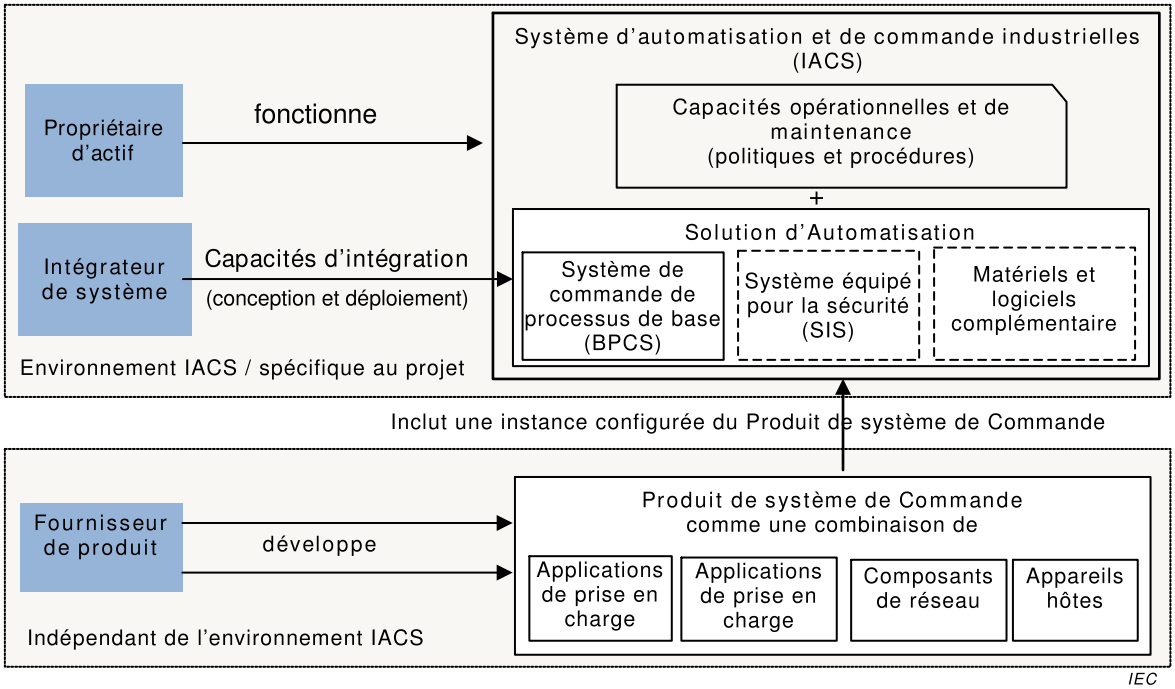

Figure 2 – Etendue des capacités du fournisseur de service

La Figure 2 représente la Solution d'Automatisation qui contient un Système de Commande de Processus de Base (BPCS), un Système Equipé pour la Sécurité (SIS) facultatif et des

Applications de Prise en Charge facultatives telles que la commande avancée. Les cases en pointillés indiquent que ces composants sont «facultatifs».

NOTE 3 Le terme «processus» dans BPCS peut s'appliquer à différents processus industriels, y compris les processus continus et les procédés de fabrication.

NOTE 4 L'Article 4.1.4 décrit les profils et la façon dont des groupes industriels et autres organisations peuvent les utiliser pour adapter la présente Norme internationale à leurs environnements spécifiques, y compris les environnements non fondés sur un IACS.

NOTE 5 En règle générale, les Solutions d'Automatisation disposent d'un seul système de commande (produit), sans toutefois s'y limiter. En général, la Solution d'Automatisation comprend l'ensemble des matériels et logiciels, indépendants de l'emballage du produit, qui est utilisé pour contrôler un processus physique (continu ou de fabrication, par exemple) tel que défini par le propriétaire d'actif.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

"Aucune référence normative"

3 Termes, définitions, abréviations et acronymes

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

3.1.1
propriétaire d'actif
individu ou organisation chargé(e) d'un ou de plusieurs IACS

Note 1 à l'article: Utilisé à la place du terme générique "utilisateur final" pour marquer la distinction.

Note 2 à l'article: Cette définition inclut les composants faisant partie intégrante de l'IACS.

Note 3 à l'article: Dans le contexte de la présente norme, le propriétaire d'actif inclut également l'opérateur de l'IACS.

3.1.2
surface d'attaque
interfaces physiques et fonctionnelles d'un système auxquelles il est possible d'accéder, et par lesquelles le système peut être potentiellement exploité

Note 1 à l'article: La taille de la surface d'attaque d'une interface logicielle est proportionnelle au nombre de méthodes et de paramètres définis pour l'interface. La surface d'attaque des interfaces simples est donc plus petite que celle des interfaces complexes.

Note 2 à l'article: La taille de la surface d'attaque et le nombre de vulnérabilités ne sont pas nécessairement corrélés.

3.1.3
Solution d'Automatisation
système de commande et tous les composants matériels et logiciels complémentaires qui ont été installés et configurés pour fonctionner dans un IACS

Note 1 à l'article: Dans la présente partie de l'IEC 62443, la Solution d'Automatisation est utilisée comme un nom propre.

Note 2 à l'article: La différence entre le système de commande et la Solution d'Automatisation est que le système de commande est intégré dans la conception de la Solution d'Automatisation (un nombre spécifique de stations de

travail, de contrôleurs et d'appareils dans une configuration spécifique, par exemple), qui est alors mise en œuvre. La configuration obtenue est appelée Solution d'Automatisation.

Note 3 à l'article: La Solution d'Automatisation peut être constituée de composants provenant de plusieurs fournisseurs, y compris d'un fournisseur de produit de système de commande.

3.1.4
système de commande de processus de base
système qui répond aux signaux d'entrée provenant du processus, de ses équipements associés, d'autres systèmes programmables et/ou d'un opérateur, et qui génère des signaux de sortie faisant fonctionner le processus et ses équipements associés de la manière souhaitée, mais qui n'exécute aucune fonction intégrée de sécurité (SIF)

Note 1 à l'article: Les fonctions équipées pour la sécurité sont spécifiées dans la série IEC 61508.

Note 2 à l'article: Le terme «processus» dans cette définition peut s'appliquer à différents processus industriels, y compris les processus continus et les procédés de fabrication.

3.1.5
consultant
sous-traitant proposant des conseils d'expertise ou des lignes directrices au fournisseur de service d'intégration ou de maintenance

3.1.6
système de commande
composants matériels et logiciels utilisés dans la conception et la mise en œuvre d'un IACS

Note 1 à l'article: Comme le représente la Figure 2, les systèmes de commande sont constitués d'appareils de terrain, d'appareils de commande intégrés, d'appareils de réseaux et d'appareils hôtes (y compris les stations de travail et les serveurs).

Note 2 à l'article: Comme l'indique la Figure 2, les systèmes de commande sont représentés dans la Solution d'Automatisation par un BPCS et un SIS facultatif.

3.1.7
transfert
transmission d'une Solution d'Automatisation au propriétaire d'actif

Note 1 à l'article: Le transfert permet effectivement au fournisseur de service d'intégration de passer la responsabilité des opérations et de la maintenance d'une Solution d'Automatisation au propriétaire d'actif, ce qui se produit en général à l'issue d'un essai système concluant, souvent appelé essai de réception sur site (ERS).

3.1.8
système d'automatisation et de commande industrielles
ensemble des personnes, matériels, logiciels, procédures et politiques impliqués dans le processus industriel et qui peuvent affecter ou influencer la sûreté, la sécurité et la fiabilité de son fonctionnement

Note 1 à l'article: L'IACS peut inclure les composants qui ne sont pas installés sur le site du propriétaire d'actif.

Note 2 à l'article: La définition de l'IACS, issue de l'IEC 62443-3-3, est représentée à la Figure 2. Des exemples d'IACS incluent les Systèmes à Commande Distribuée (DCS) et les Systèmes de Commande, Surveillance et Acquisition de Données (SCADA). L'IEC 62443-2-4 définit également la "Solution" en nom propre pour signifier l'instance spécifique du produit de système de commande et la possibilité de composants supplémentaires conçus dans l'IACS. La Solution d'Automatisation est donc différente du système de commande, étant donné qu'elle représente une mise en œuvre particulière (conception et configuration) des composants matériels et logiciels du système de commande pour un propriétaire d'actif spécifique.

3.1.9
fournisseur de service d'intégration
fournisseur de service qui propose des activités d'intégration d'une Solution d'Automatisation, y compris la conception, l'installation, la configuration, les essais, la mise en service et le transfert

Note 1 à l'article: Les fournisseurs de service d'intégration sont souvent appelés intégrateurs ou sous-traitants principaux d'automatisation (MAC).

3.1.10
fournisseur de service de maintenance
fournisseur de service qui propose des activités de support pour une Solution d'Automatisation après transfert

Note 1 à l'article: La maintenance est souvent différenciée de l'exploitation (par exemple, le langage familier courant estime souvent qu'une Solution d'Automatisation est probablement en exploitation ou en maintenance). Les fournisseurs de service de maintenance peuvent réaliser des activités de support au cours des opérations, par exemple, la gestion des comptes utilisateurs, la surveillance de la sécurité et les évaluations de sécurité.

3.1.11
support portable
appareils portables contenant des capacités de stockage des données, pouvant être utilisés pour copier physiquement des données à partir d'un élément de matériel et les transférer à un autre

Note 1 à l'article: Les types de supports portables incluent, sans toutefois s'y limiter: lecteur CD/DVD/BluRay Media, périphériques de stockage USB, téléphones intelligents, mémoire flash, disques électroniques, disques durs, ordinateurs de poche et ordinateurs portables.

3.1.12
fournisseur de produit
fabricant de produit matériel et/ou logiciel

Note 1 à l'article: Utilisé à la place du terme générique "fournisseur" pour marquer la distinction.

3.1.13
accès distant
accès à un système de commande par une interface externe du système de commande

Note 1 à l'article: Les exemples d'applications qui prennent en charge l'accès distant comprennent RDP, OPC et Syslog.

Note 2 à l'article: En général, les applications d'accès distant et la Solution d'Automatisation sont placées dans des zones de sécurité différentes déterminées par le propriétaire d'actif. Voir l'IEC 62443-3-2 pour l'application des zones et des conduits à la Solution d'Automatisation par le propriétaire d'actif.

3.1.14
système équipé pour la sécurité
système utilisé pour la mise en œuvre de la sécurité fonctionnelle

Note 1 à l'article: Voir l'IEC 61508 et l'IEC 61511 pour plus d'informations sur la sécurité fonctionnelle.

3.1.15
faille de sécurité
violation de la sécurité d'un système telle qu'une (1) divulgation ou modification non autorisée d'informations ou (2) un refus de service est susceptible de s'être produit(e)

Note 1 à l'article: Une faille de sécurité représente une violation de la sécurité d'un système ou une infraction à ses politiques de sécurité. Elle est indépendante de l'impact ou de l'impact potentiel du système.

3.1.16
incident de sécurité
faille de sécurité revêtant une certaine importance pour le propriétaire d'actif ou tentative infructueuse de compromettre le système dont le résultat aurait pu revêtir une certaine importance pour le propriétaire d'actif

Note 1 à l'article: Le terme "d'une certaine importance" se rapporte à l'environnement dans lequel la faille de sécurité est détectée. Par exemple, la même faille peut être déclarée comme incident de sécurité dans un environnement et pas dans un autre. Les activités de tri sont souvent utilisées par les propriétaires d'actif pour évaluer les failles de sécurité et identifier celles qui sont suffisamment importantes pour être considérées comme des incidents.

Note 2 à l'article: Dans certains environnements, les tentatives infructueuses de compromettre le système, telles que les tentatives de connexion infructueuses, sont considérées comme suffisamment importantes pour être classées comme des incidents de sécurité.

3.1.17
correctif de sécurité
correctif logiciel pertinent pour la sécurité d'un composant logiciel

Note 1 à l'article: Pour les besoins de cette définition, un micrologiciel est considéré comme un logiciel.

Note 2 à l'article: Les correctifs logiciels peuvent résoudre les vulnérabilités connues ou potentielles, ou tout simplement améliorer la sécurité du composant logiciel, y compris la fiabilité de son fonctionnement.

3.1.18
programme de sécurité
portefeuille des services de sécurité, y compris les services d'intégration et les services de maintenance, et leurs politiques, procédures et produits connexes qui sont applicables à l'IACS

Note 1 à l'article: Le programme de sécurité pour les fournisseurs de service IACS se rapporte aux politiques et procédures qu'ils ont définies pour résoudre les problèmes de sécurité de l'IACS.

3.1.19
fournisseur de service
individu ou organisation (organisation interne ou externe, fabricant, etc.) qui fournit un service de support spécifique et des fournitures associées en vertu d'un accord avec le propriétaire d'actif

Note 1 à l'article: Ce terme est utilisé à la place du terme générique "fournisseur" pour marquer la distinction.

3.1.20
sous-traitant
fournisseur de service sous contrat avec le fournisseur de service d'intégration ou de maintenance ou avec un autre sous-traitant directement ou indirectement sous contrat avec le fournisseur de service d'intégration ou de maintenance

3.1.21
système
éléments interdépendants formant un tout complexe

Note 1 à l'article: Un système peut être emballé comme un produit.

Note 2 à l'article: Dans la pratique, l'utilisation d'un adjectif permet souvent de clarifier l'interprétation de sa signification (un système de commande, par exemple). Dans le contexte d'un système de commande, les éléments sont en grande partie des éléments matériels et logiciels.

3.1.22
vérification
contrôle permettant de vérifier que l'exigence spécifiée a été satisfaite

3.1.23
vulnérabilité
faille ou faiblesse dans la conception, la mise en œuvre ou l'exploitation et la gestion d'un composant qui peut être exploitée pour causer une faille de sécurité

Note 1 à l'article: En règle générale, les politiques de sécurité incluent généralement des politiques de protection de la confidentialité, de l'intégrité et de la disponibilité des actifs du système.

3.2 Abréviations

AES_GCM Advanced Encryption Standard Galois/Counter Mode (Norme de chiffrement avancé, Mode de comptoir galois)

BPCS Basic Process Control System (système de commande de processus de base)

BR	Base Requirement (exigence de base)
CEF	Common Event Format (format d'événements commun)
DCOM	Distributed Common Object Model (modèle d'objet commun distribué)
DCS	Distributed Control System (système à commande distribuée)
EWS	Engineering Workstation (station de travail technique)
IACS	Industrial Automation and Control System (système d'automatisation et de commande industrielles)
RE	Requirement Enhancement (amélioration d'exigence)
RDP	Remote Desktop Protocol (protocole de bureau à distance)
RFC	Request For Comment (demande de commentaires)
RFQ	Request For Quote (demande d'appels d'offres)
SCADA	Supervisory Control And Data Acquisition (système de commande, surveillance et acquisition de données).
SIEM	Security Information and Event Management (gestion des informations et événements de sécurité)
SIF	Safety Instrumented Function (fonction équipée pour la sécurité)
SIL	Safety Integrity Level (niveau d'intégrité de sécurité)
SIS	Safety Instrumented System (système équipé pour la sécurité)
SNMP	Simple Network Management Protocol (protocole simple de gestion de réseau)
SOW	Statement Of Work (énoncé des travaux)
SSID	Service Set Identifier (Identificateur d'ensemble de service)
SP	Security Program (programme de sécurité)
TR	Technical Report (rapport technique)
VPN	Virtual Private Network (réseau privé virtuel)

4 Concepts

4.1 Utilisation de l'IEC 62443-2-4

4.1.1 Utilisation de l'IEC 62443-2-4 par les fournisseurs de service IACS

La présente partie de la série IEC 62443 définit les exigences pour la prise en charge des capacités de sécurité par des programmes de sécurité des fournisseurs de service d'intégration et de maintenance (voir 4.1.3 et 4.1.6). La prise en charge de ces capacités signifie que le fournisseur de service peut les fournir au propriétaire d'actif, sur demande. Les termes et conditions de fourniture de ces capacités ne relèvent pas du domaine d'application de la présente norme. En outre, l'IEC 62443-2-4 peut être utilisée par ces fournisseurs de service IACS pour structurer et améliorer leurs programmes de sécurité.

De plus, les fournisseurs de service IACS peuvent utiliser l'IEC 62443-3-3 et l'IEC 62443-4-2 conjointement avec l'IEC 62443-2-4 pour travailler avec les fournisseurs de systèmes de commande/composants sous-jacents. Cette collaboration peut aider le fournisseur de service à développer des politiques et des procédures autour d'une capacité d'un système/composant (la sauvegarde et la restauration basées sur les recommandations des fournisseurs des systèmes/composants utilisés, par exemple).

Il est prévu que les programmes de sécurité qui mettent en œuvre ces exigences soient indépendants des différentes versions du système de commande intégré dans la Solution d'Automatisation. Ceci signifie qu'une nouvelle version du produit de système de commande n'exige pas nécessairement de modifier le programme de sécurité du fournisseur de service. Cependant, les modifications apportées au programme de sécurité sont exigées lorsque les modifications apportées au système de commande sous-jacent ont une incidence préjudiciable sur la conformité du programme de sécurité existant aux exigences de l'IEC 62443-2-4.

EXEMPLE 1 Un fournisseur de service peut être expérimenté sur une ligne spécifique de produits du système de commande. L'élaboration de politiques et de procédures pour cette ligne de produits est basée sur les recommandations du fournisseur de produit et les capacités de la ligne de produits. Par conséquent, lorsque les capacités de produit en matière de sauvegarde et de restauration sont modifiées, il peut s'avérer nécessaire de modifier les capacités correspondantes du programme de sécurité du fournisseur de service (correspondant à SP.12.XX) pour conserver la cohérence avec les capacités de produit actualisées. D'autre part, les politiques et procédures du fournisseur de service relatives aux accords de confidentialité ou aux vérifications des antécédents du personnel (correspondant à SP.01.03 et SP.01.04) ne dépendent très probablement pas du produit de système de commande utilisé dans la Solution d'Automatisation.

Cette collaboration peut également permettre d'améliorer la sécurité dans ces systèmes/composants. En premier lieu, le fournisseur de service peut recommander des fonctions de sécurité nouvelles ou mises à jour au fournisseur du système/composant. En second lieu, le fournisseur de service peut acquérir des connaissances sur le système/composant, lui permettant d'ajouter ses propres mesures de sécurité compensatoires à la Solution d'Automatisation lors du déploiement ou de la maintenance.

Les exigences sont spécifiées à l'Annexe A et sont définies en termes de capacités que ces programmes de sécurité ont à fournir. L'Article 4.1.4 présente l'aptitude des groupes industriels à intégrer ces capacités dans des profils pour réduire les risques. Voir l'IEC 62443-3-2 pour plus de détails sur les risques de sécurité.

L'IEC 62443-2-4 reconnaît également que les programmes de sécurité évoluent et que les capacités suivent leur propre cycle de vie, commençant souvent de manière totalement manuelle et évoluant au fil du temps pour devenir plus formelles, plus cohérentes et plus efficaces. L'Article 4.2 aborde cette question des capacités d'évolution en définissant un modèle de maturité à utiliser avec l'application de la présente norme.

EXEMPLE 2 Une capacité spécifique peut être introduite sous la forme d'un ensemble de procédures manuelles, puis ultérieurement complétée par des outils automatisés.

En conséquence, les exigences de l'Annexe A sont établies de manière abstraite pour un large éventail de mises en œuvre. Il est prévu que les fournisseurs de service et les propriétaires d'actif négocient et conviennent des capacités exigées à fournir et de la manière dont elles sont à fournir. Ces aspects visant à satisfaire aux exigences ne relèvent pas du domaine d'application de l'IEC 62443-2-4, même s'il convient que l'utilisation de profils en facilite la tâche.

EXEMPLE 3 Un fournisseur de service en mesure de prendre en charge des mots de passe complexes est tenu de pouvoir prendre en charge des variations spécifiques de mots de passe complexes telles que définies par les politiques de mot de passe des propriétaires d'actif.

EXEMPLE 4 De nombreuses capacités présentent un aspect opportun lié à leurs performances. Il convient que les éléments considérés comme étant opportuns fassent l'objet d'un accord entre le propriétaire d'actif et le fournisseur de service.

4.1.2 Utilisation de l'IEC 62443-2-4 par les propriétaires d'actif IACS

L'IEC 62443-2-4 peut être utilisée par les propriétaires d'actif pour demander des capacités de sécurité spécifiques auprès du fournisseur de service. Plus précisément, avant une telle demande, les propriétaires d'actif peuvent utiliser l'IEC 62443-2-4 pour déterminer si le programme de sécurité d'un fournisseur de service particulier comprend ou non les capacités dont a besoin le propriétaire d'actif.

En général, l'IEC 62443-2-4 reconnaît que les exigences des propriétaires d'actif varient. Elle a donc été élaborée pour encourager les fournisseurs de service à mettre en œuvre les capacités exigées afin qu'elles puissent être adaptées à un large éventail de propriétaires d'actif. Le modèle de maturité permet également aux propriétaires d'actif de mieux comprendre la maturité des capacités d'un fournisseur de service particulier.

4.1.3 Utilisation de l'IEC 62443-2-4 lors de négociations entre des propriétaires d'actif et des fournisseurs de service IACS

Avant que le fournisseur de service IACS ne commence à travailler sur la Solution d'Automatisation, le propriétaire d'actif émet généralement un appel d'offres (RFQ) comprenant un document (par exemple, un énoncé des travaux (SOW)) qui définit ses politiques et exigences de sécurité, y compris les exigences spécifiées à l'Annexe A qui s'appliquent. Voir l'IEC 62443-3-2 pour de plus amples informations sur la définition des exigences de sécurité. Les fournisseurs de service répondent à l'appel d'offres (RFQ) et entament des négociations à l'issue desquelles le fournisseur de service et le propriétaire d'actif conviennent des détails de l'énoncé des travaux (SOW) (ou un document similaire). En règle générale, les responsabilités et capacités spécifiques du fournisseur de service en termes de prise en charge des politiques et des exigences de sécurité du propriétaire d'actif sont incluses dans ou référencées par cet accord / contrat entre le fournisseur de service IACS et le propriétaire d'actif.

NOTE 1 Un contrat de ce type peut ne pas être nécessaire lorsque le fournisseur de service fait partie de l'organisation du propriétaire d'actif.

En outre, le propriétaire d'actif ne précise généralement pas la façon dont ses exigences de sécurité (sauvegarde et restauration, par exemple) seront mises en œuvre, ceci ayant déjà été spécifié par le fournisseur de service dans ses politiques et procédures. Toutefois, le propriétaire d'actif peut définir les contraintes et les paramètres (valeurs de délai d'expiration de mot de passe, par exemple) d'application des politiques et procédures du fournisseur de service dans son projet spécifique.

Lorsque le propriétaire d'actif ne spécifie pas d'exigences de sécurité, le fournisseur de service peut lui en proposer en fonction de sa propre analyse de sécurité, et ensuite négocier celles qui sont incluses dans le SOW.

Il est également prévu que le fournisseur de service IACS présente certaines aptitudes à personnaliser ses capacités à satisfaire aux besoins du propriétaire d'actif. Toutefois, la spécification de cette personnalisation ne relève pas du domaine d'application de l'IEC 62443-2-4.

4.1.4 Profils

Les profils sont des ensembles de capacités définies par la sélection d'un sous-ensemble spécifique des exigences spécifiées à l'Annexe A. Les profils sont destinés à être rédigés pour les différents groupes / secteurs industriels et d'autres organisations pour définir un ou plusieurs ensembles de capacités plus appropriés à leurs besoins.

Les rapports techniques (TR) de l'IEC peuvent être créés par des groupes / secteurs industriels ou d'autres organisations pour définir des profils. Chaque TR peut définir un ou plusieurs profils, et chaque profil identifie un sous-ensemble des exigences définies à l'Annexe A.

Il est prévu que les propriétaires d'actif choisissent des profils existants pour spécifier les exigences dont ils ont besoin pour leurs Solutions d'Automatisation.

4.1.5 Fournisseurs de service d'intégration IACS

Un fournisseur de service d'intégration IACS est une organisation, en général distincte du propriétaire d'actif et sous contrat avec ce dernier, qui fournit des capacités de mise en œuvre/déploiement de Solutions d'Automatisation en fonction des exigences du propriétaire d'actif. En règle générale, les activités du fournisseur de service d'intégration se déroulent dans le calendrier commençant par la phase de conception et finissant avec le transfert de la Solution d'Automatisation au propriétaire d'actif.

NOTE 1 Le fournisseur de service d'intégration peut être une organisation dans l'organisation du propriétaire d'actif.

En règle générale, les activités du fournisseur de service d'intégration IACS incluent:

a) l'analyse de l'environnement physique, électrique ou mécanique que la Solution d'Automatisation a à contrôler (le processus physique à contrôler, comme ceux utilisés dans les procédés de fabrication, d'affinage ou pharmaceutiques, par exemple),

b) le développement d'une architecture de Solution d'Automatisation en termes d'appareils et de boucles de commande, ainsi que leur interconnectivité avec les stations de travail techniques et de l'opérateur, et éventuellement l'inclusion d'un système équipé pour la sécurité (SIS),

c) la définition de la manière dont la Solution d'Automatisation se connecte à des réseaux (une usine, par exemple) externes,

d) l'installation, la configuration, l'application de correctifs, la sauvegarde et les essais amenant au transfert de la Solution d'Automatisation au propriétaire d'actif pour l'exploitation.

e) l'obtention de l'approbation du propriétaire d'actif pour la plupart des décisions prises et les résultats générés lors de l'exécution de ces activités.

Cette description des activités du fournisseur de service d'intégration est abstraite et peut exclure certaines de ces activités ou en inclure d'autres qui en général précèdent le transfert de la Solution d'Automatisation. De même, ces activités incluent la participation du propriétaire d'actif pour s'assurer que ses exigences sont satisfaites.

Du point de vue de l'IEC 62443, les fournisseurs de service d'intégration sont également censés participer à l'appréciation des risques de sécurité pour la Solution d'Automatisation ou utiliser les résultats de ce type d'évaluation fournie par le propriétaire d'actif. Le fournisseur de service est également censé utiliser les capacités exigées par l'IEC 62443-2-4 dans son programme de sécurité pour traiter ces risques.

NOTE 2 Voir l'IEC 62443-3-2 pour des lignes directrices sur l'utilisation des appréciations du risque et la définition des exigences de sécurité.

4.1.6 Fournisseurs de service de maintenance IACS

Un fournisseur de service de maintenance IACS est toute organisation, en général distincte du propriétaire d'actif et sous contrat avec ce dernier, qui effectue des activités de maintenance et d'entretien des Solutions d'Automatisation en fonction des exigences du propriétaire d'actif.

Les activités de maintenance sont distinctes des activités destinées au fonctionnement de la Solution d'Automatisation et sont généralement classées en deux catégories: les activités qui s'appliquent spécifiquement au maintien de la sécurité de la Solution d'Automatisation, et les activités qui s'appliquent au maintien d'autres aspects de la Solution d'Automatisation, tels que la maintenance de l'appareil et du matériel, mais qui impliquent de s'assurer que la sécurité n'est pas dégradée du fait de ces activités.

NOTE 1 Le fournisseur de service de maintenance peut être une organisation dans l'organisation du propriétaire d'actif.

NOTE 2 Un ou plusieurs fournisseurs de service de maintenance de la Solution d'Automatisation peuvent intervenir en même temps ou l'un après l'autre.

Les activités de maintenance commencent généralement après le transfert de la Solution d'Automatisation au propriétaire d'actif et peuvent se poursuivre tant que le propriétaire d'actif le demande. Elles sont généralement de courte durée et souvent récurrentes, et comprennent en règle générale un ou plusieurs des éléments suivants:

a) les mises à jour de correctif et des antivirus,

b) les mises à niveau et la maintenance du matériel, y compris les petits réglages techniques non liés directement aux algorithmes de contrôle,

c) la migration des composants et du système,

d) la gestion des modifications,

e) la gestion du plan de secours.

Toutes les activités de maintenance comprennent un certain niveau de sensibilisation à la sécurité indépendamment du fait qu'elles soient directement liées ou non à la sécurité. Il convient qu'aucune activité, une fois réalisée, ne réduise le niveau de sécurité.

Cette description des activités de maintenance est abstraite et peut inclure d'autres activités qui en général suivent le transfert de la Solution d'Automatisation. De même, ces activités incluent la participation du propriétaire d'actif pour s'assurer que ses exigences sont satisfaites.

Du point de vue de la série IEC 62443, les fournisseurs de service de maintenance, comme les fournisseurs de service d'intégration, sont censés participer à l'appréciation des risques de sécurité pour la Solution d'Automatisation (comme ceux correspondant aux modifications proposées) ou utiliser les résultats de ce type d'évaluation fournie par le propriétaire d'actif. Le fournisseur de service est également censé utiliser les capacités exigées par l'IEC 62443-2-4 dans son programme de sécurité pour traiter ces risques.

NOTE 3 Voir l'IEC 62443-3-2 pour des lignes directrices sur l'utilisation des appréciations des risques et la définition des exigences de sécurité.

4.2 Modèle de maturité

Les exigences spécifiées à l'Annexe A se prêtent à de nombreuses interprétations quant à la manière dont elles peuvent être fournies par un fournisseur de service. Le présent article définit un modèle de maturité qui définit les repères permettant de satisfaire à ces exigences.

Ces repères sont définis par des niveaux de maturité, comme indiqués au Tableau 1. Les niveaux de maturité reposent sur le modèle CMMI-SVC, défini dans CMMI® for Services, Version 1.3. La colonne *Description/Comparaison avec CMMI-SVC* du Tableau 1 présente les relations avec CMMI-SVC.

Chaque niveau est progressivement plus avancé que le niveau précédent, et s'applique indépendamment pour chaque exigence du Tableau A.1. Les fournisseurs de service ont à identifier le niveau de maturité associé à leur mise en œuvre de chaque exigence. Les propriétaires d'actif peuvent également déterminer, en termes mesurables, le niveau de maturité des capacités d'un fournisseur de service particulier.

Ce modèle s'applique aux exigences de base (BR) et aux améliorations d'exigences (RE) définies au Tableau A.1. Les améliorations d'exigences de ce tableau sont des extensions d'exigences de base et ne reflètent pas la maturité. Les améliorations d'exigences sont plutôt définies pour fournir des spécialisations, des restrictions ou des généralisations d'exigences de base. Elles sont utilisées de la même manière que dans l'IEC 62443-3-3.

NOTE 1 Les groupes/secteurs industriels peuvent identifier les niveaux de maturité spécifiques de chacun pour mieux satisfaire à leurs besoins individuels.

NOTE 2 Il est prévu que, dans le temps et pour une exigence particulière, les capacités d'un fournisseur de service évoluent à des niveaux plus élevés au fur et à mesure des progrès réalisés pour satisfaire aux exigences.

Tableau 1 – Niveaux de maturité

Niveau	CMMI-SVC	IEC 62443-2-4	Description/Comparaison avec CMMI-SVC de l'IEC 62443-2-4
1	Initial	Initial	À ce niveau, les modèles sont foncièrement identiques. En règle générale, les fournisseurs de service exécutent le service de manière ponctuelle et souvent non documentée (ou pas totalement documentée). Les exigences pour le service sont en général spécifiées dans un énoncé des travaux dans le cadre d'un contrat avec le propriétaire d'actif. La cohérence entre les projets peut donc ne pas être révélée. NOTE Dans ce contexte, le terme "documenté" fait référence à la procédure d'exécution de ce service (les instructions détaillées adressées au personnel du fournisseur de service, par exemple) et non pas aux résultats de son exécution. Dans la plupart des paramètres du propriétaire d'actif, toutes les modifications résultant de l'exécution des services sont documentées.
2	Géré	Géré	À ce niveau, les modèles sont foncièrement identiques, sauf que l'IEC 62443-2-4 reconnaît la possible existence d'un délai significatif entre la définition d'un service et son exécution (sa mise en pratique). Par conséquent, les aspects liés à l'exécution de CMMI-SVC Niveau 2 sont reportés au Niveau 3. À ce niveau, le fournisseur de service a la capacité de gérer la fourniture et l'exécution du service conformément aux politiques définies (y compris les objectifs). Le fournisseur de service dispose également d'éléments probants permettant de montrer que le personnel est compétent, formé et/ou capable de suivre les procédures écrites d'exécution du service. La discipline de service reflétée par le Niveau de maturité 2 aide à s'assurer que les pratiques liées au service sont répétables, même en période de stress. Lorsque ces pratiques sont en place, elles sont exécutées et gérées selon leurs plans documentés.
3	Défini	Défini (mis en pratique)	À ce niveau, les modèles sont foncièrement identiques, sauf que les aspects liés à l'exécution de CMMI-SVC Niveau 2 sont inclus ici. Par conséquent, un service au Niveau 3 est un service de Niveau 2 que le fournisseur de service a mis en pratique au moins une fois pour un propriétaire d'actif. Les performances d'un service de Niveau 3 peuvent être présentées comme étant répétables dans une organisation du fournisseur de service. Les services de Niveau 3 peuvent être adaptés à des projets individuels en fonction du contrat et de l'énoncé des travaux provenant du propriétaire d'actif.
4	Quantitativement géré	Amélioration	À ce niveau, la Partie 2-4 combine les niveaux 4 et 5 de CMMI-SVC. Grâce à des mesures de processus adaptées, les fournisseurs de service contrôlent l'efficacité et les performances du service, et démontrent les améliorations continues dans ces domaines, telles que des procédures plus efficaces ou l'installation de capacités de système présentant des niveaux de sécurité plus élevés (voir l'IEC 62443-3-3). Cela donne lieu à un programme de sécurité qui améliore le service par des modifications de technologie/procédure/gestion. Voir l'IEC 62443-1-3 pour une présentation des mesures.
5	Optimisation		

5 Aperçu des exigences

5.1 Sommaire

L'Annexe A contient la liste des exigences de programme de sécurité pour les fournisseurs de service d'intégration et de maintenance IACS. Elles sont spécifiées sous la forme d'une liste d'exigences de base (BR) et d'améliorations d'exigences (RE) présentées au Tableau A.1. Les BR et les RE sont décrites en 5.5.2. Chacune spécifie une capacité que le fournisseur de service peut offrir au propriétaire d'actif lors des activités d'intégration et de maintenance.

NOTE Les groupes/secteurs industriels peuvent définir des sous-ensembles d'exigences pour mieux satisfaire à leurs besoins individuels.

5.2 Tri et filtrage

Les colonnes du Tableau A.1 ont été conçues pour être aisément triées et filtrées électroniquement en utilisant la version de feuille de calcul du tableau fournie avec la présente norme internationale. Cela permet à différents lecteurs d'organiser les exigences en fonction de leurs besoins. Les valeurs de colonne utilisées pour le tri et le filtrage sont définies en 5.5.

5.3 Modèle de hiérarchie de l'IEC 62264-1

La plupart des exigences de l'Annexe A se rapportent au réseau ou aux niveaux d'application dans des phrases telles que "un appareil portatif sans fil est utilisé au Niveau 2". En lettres majuscules, "Niveau" est utilisé dans ce contexte en référence à la position dans l'IEC 62264-1. Le modèle de zones et conduits décrit par l'IEC 62443-3-2 est référencé par les exigences spécifiées à l'Annexe A qui traitent, indépendamment du Niveau de modèle de hiérarchie de l'IEC 62264-1, de la définition des limites de confiance qui subdivisent la Solution d'Automatisation en partitions dénommées «zones» par l'IEC 62443-3-2.

NOTE Le modèle de hiérarchie de l'IEC 62264-1 est également désigné Modèle de Référence Purdue (PRM – Purdue Reference Model) et est également spécifié par l'ISA 95.

5.4 Colonnes du tableau des exigences

Les colonnes utilisées au Tableau A.1 sont définies au Tableau 2. Les valeurs de ces colonnes sont définies en 5.5.

Tableau 2 – Colonnes

Colonne	Description de la colonne
ID req	Identificateur d'exigence
BR/RE	Exigence de base/Indicateur d'amélioration d'exigence
Zone fonctionnelle	Mot-clé représentant la principale zone fonctionnelle d'une exigence
Sujet	Mot-clé représentant le sujet principal associé à une exigence. Le même sujet peut s'appliquer à plusieurs zones fonctionnelles.
Sous-sujet	Mot-clé représentant le sous-sujet concerné par l'exigence. Le même sujet technique peut s'appliquer à plusieurs zones fonctionnelles et/ou activités.
Doc?	La documentation livrable est à fournir au propriétaire d'actif (oui/non). NOTE Certaines exigences peuvent exiger que le fournisseur de service gère la documentation qui n'est pas considérée comme étant livrable. Toutefois, le fournisseur de service peut présenter ou livrer cette documentation au propriétaire d'actif dans le cadre d'un contrat.
Description de l'exigence	Texte de l'exigence.
Justification	Texte décrivant le contexte, la justification et d'autres aspects de l'exigence pour faciliter la compréhension du lecteur.

5.5 Définitions des colonnes

5.5.1 Colonne ID Req

Cette colonne contient l'identificateur d'exigences de programme de sécurité. Le même ID Req identifie une exigence de base et ses améliorations d'exigences. Cet identificateur est structuré en trois parties séparées par des points (".") :

- la première partie est "SP", indiquant le "Programme de sécurité";

- la deuxième partie est l'identificateur à deux chiffres pour la zone fonctionnelle (voir Tableau 3 pour les valeurs);
- la troisième partie est l'identificateur à deux chiffres pour l'exigence, attribué de manière numérique dans la zone fonctionnelle. Les exigences de base et leurs améliorations d'exigences présentent toutes le même identificateur d'exigence SP. Voir 5.5.2 pour la description des exigences de base et des améliorations d'exigences.

5.5.2 Colonne BR/RE

Cette colonne indique si l'exigence est une exigence de base (BR) ou une amélioration d'exigence (RE).

Exigences de base

Les exigences de base sont considérées comme étant des exigences fondamentales pour tous les programmes de sécurité. Elles sont en général abstraites par nature, pour laisser toute la latitude aux fournisseurs de service dans leur mise en œuvre.

Améliorations d'exigences

Les améliorations d'exigences imposent en général des restrictions, ou autres spécialisations, sur les capacités des exigences de base ou des exigences améliorées. Les améliorations d'exigences reposant sur des exigences de base offrent un niveau de restriction/spécialisation d'exigence de base, alors que les améliorations d'exigences reposant sur d'autres améliorations d'exigences offrent des niveaux de restrictions/spécialisations plus élevés sur l'exigence de base. Ces restrictions/spécialisations ont pour objet d'améliorer la sécurité grâce à une application plus sophistiquée ou plus rigoureuse des capacités de sécurité.

Mise en œuvre d'exigence

En conséquence, un fournisseur de service qui met en œuvre une capacité définie par une exigence de base peut choisir un large éventail de mises en œuvre pour satisfaire à l'exigence. D'autre part, un fournisseur de service qui met en œuvre une capacité définie par une amélioration d'exigence dispose d'une plage limitée de mises en œuvre.

Numérotation d'exigence

Les exigences de base et ses améliorations partagent le même ID Req SP (voir 5.5.1). Les améliorations d'exigences sont numérotées dans l'ordre, en commençant par 1 pour chaque exigence de base.

Les améliorations d'exigences (RE) sont numérotées dans l'ordre en commençant par 1 pour chaque exigence de base, et ce numéro de séquence est placé entre parenthèses après RE. Par conséquent, la valeur de la colonne est RE(#), où # est le numéro de séquence de l'amélioration. Les numéros des améliorations d'exigences qui en améliorent d'autres sont supérieurs aux améliorations qu'elles améliorent.

EXEMPLE 1 Le SP.01.02 BR est une exigence de base permettant d'affecter à la Solution d'Automatisation du personnel ayant été informé des exigences de sécurité de l'IEC 62443-2-4, et le RE(1) améliore cette exigence en définissant une exigence de vérification des antécédents du personnel du fournisseur de service affecté à la Solution d'Automatisation. L'exigence de base stipule que le fournisseur de service peut affecter à la Solution d'Automatisation quiconque a été formé sur les exigences de l'IEC 62443-2-4, alors que RE(1) stipule qu'il peut uniquement affecter du personnel formé ayant satisfait aux vérifications des antécédents.

EXEMPLE 2 Le SP.01.02 RE(2) définit une amélioration pour l'exigence RE(1) en spécialisant l'exigence RE(1) à appliquer au personnel sous-traitant affecté à la Solution d'Automatisation.

5.5.3 Colonne Zone fonctionnelle

Cette colonne fournit l'organisation de niveau supérieur des exigences. Le Tableau 3 donne une liste des zones fonctionnelles.

Tableau 3 – Valeurs de la colonne Zone fonctionnelle

Valeur	ID Req SP	Description
Affectation en personnel pour la Solution	SP.01.XX	Exigences relatives à l'affectation de personnel aux activités liées à la Solution d'Automatisation par le fournisseur de service.
Assurance	SP.02.XX	Exigences visant à garantir la réalisation de la politique de sécurité de la Solution d'Automatisation
Architecture	SP.03.XX	Exigences relatives à la conception de la Solution d'Automatisation
Sans fil	SP.04.XX	Exigences relatives à l'utilisation d'un système sans fil dans la Solution d'Automatisation
SIS	SP.05.XX	Exigences relatives à l'intégration d'un système équipé pour la sécurité (SIS) dans la Solution d'Automatisation
Gestion de la configuration	SP.06.XX	Exigences relatives au contrôle de la configuration de la Solution d'Automatisation
Accès distant	SP.07.XX	Exigences relatives à l'accès distant à la Solution d'Automatisation
Gestion des événements	SP.08.XX	Exigences relatives à la gestion des événements dans la Solution d'Automatisation
Gestion des comptes	SP.09.XX	Exigences relatives à l'administration des comptes utilisateur dans la Solution d'Automatisation
Protection contre les logiciels malveillants	SP.10.XX	Exigences relatives à l'utilisation d'un logiciel anti logiciels malveillants dans la Solution d'Automatisation
Gestion des correctifs	SP.11.XX	Exigences relatives aux aspects liés à la sécurité de l'approbation et de l'installation de correctifs logiciels
Sauvegarde/Restauration	SP.12.XX	Exigences relatives aux aspects liés à la sécurité de la sauvegarde et la restauration

5.5.4 Colonne Sujet

Cette colonne contient le mot-clé qui décrit le mieux le sujet principal traité par l'exigence. Les mots-clés de sujet sont indépendants des zones fonctionnelles permettant d'utiliser le filtrage et rechercher toutes les exigences appartenant au même sujet, quelle que soit la zone fonctionnelle. Le Tableau 4 fournit une liste des valeurs pour cette colonne.

Tableau 4 – Valeurs de la colonne Sujet

Valeur	Description
Comptes – …	Exigences relatives aux différents types de comptes utilisateurs
Outils et logiciels de sécurité	Exigences relatives aux logiciels et outils d'application utilisés dans la Solution d'Automatisation à des fins de sécurité
Vérifications des antécédents	Exigences relatives aux vérifications des antécédents
Sauvegarde	Exigences relatives aux sauvegardes et à la restauration de la Solution d'Automatisation après sauvegarde
Protection des données	Exigences relatives à la protection des données
Appareils – …	Exigences relatives aux différents types d'appareils utilisés dans la Solution d'Automatisation
Événements – …	Exigences relatives aux différents types d'événements utilisés dans la Solution d'Automatisation (Sécurité, failles de sécurité, alarmes et événements, par exemple)
Lignes directrices de renforcement	Exigences relatives aux lignes directrices permettant de renforcer la Solution d'Automatisation
Processus manuel	Exigences relatives aux procédures manuelles utilisées pour fournir les capacités liées à la sécurité (gestion des correctifs, sauvegarde/restauration, par exemple)
Conception du réseau	Exigences relatives à la conception de l'architecture réseau de la Solution d'Automatisation
Mots de passe	Exigences relatives aux mots de passe du compte
Liste des correctifs	Exigences relatives à une liste d'identificateurs et de propriétés des correctifs de sécurité applicables à la Solution d'Automatisation
Affectations de personnel	Exigences relatives à l'affectation de personnel à la Solution d'Automatisation
Support portable	Exigences relatives à l'utilisation d'un support portable dans la Solution d'Automatisation
Restauration	Exigences relatives à la restauration de la Solution d'Automatisation après sauvegarde
Appréciation du risque	Exigences relatives aux appréciations des risques pour la Solution d'Automatisation et ses composants
Outils et logiciels de sécurité	Exigences relatives aux outils/logiciels utilisés pour la mise en œuvre et la gestion de la sécurité dans la Solution d'Automatisation
Composants de Solution	Exigences relatives aux composants utilisés dans la Solution d'Automatisation
Formation	Exigences relatives à la formation du personnel affecté à la Solution d'Automatisation
Interface utilisateur	Exigences relatives aux interfaces utilisateurs de la Solution d'Automatisation
Vulnérabilités	Exigences relatives aux vulnérabilités de sécurité dans la Solution d'Automatisation

5.5.5 Colonne Sous-sujet

Cette colonne contient le mot-clé qui décrit le mieux le sujet technique associé à l'exigence. Les mots-clés de sujet technique sont indépendants des zones fonctionnelles et des activités permettant d'utiliser le filtrage et rechercher toutes les exigences appartenant au même sujet technique, quelle que soit la zone fonctionnelle ou l'activité. Le Tableau 5 fournit une liste des valeurs pour cette colonne.

Tableau 5 – Valeurs de la colonne Sous-sujet

Valeur	Description
Contrôle d'accès	Exigences relatives à l'authentification et/ou aux autorisations
Administration	Exigences relatives aux activités d'administration et de gestion (administration de l'appareil et gestion des comptes, par exemple)
Approbation	Exigences relatives à l'obtention des approbations auprès du propriétaire d'actif
Modification	Exigences relatives à la modification des mots de passe
Communications	Exigences relatives aux communications internes et externes de la Solution d'Automatisation
Composition	Exigences relatives à la composition des mots de passe
Mode de configuration	Exigences relatives à l'état d'un appareil lui permettant d'être configuré
Connectivité	Exigences relatives à la connectivité réseau des appareils et/ou segments de réseau
Cryptographie	Exigences relatives à l'utilisation des mécanismes cryptographiques (chiffrement, signatures numériques, par exemple)
Rétention de données / d'événements	Exigences relatives à l'archivage des données et événements
Livraison	Exigences relatives à la livraison des correctifs
Détection	Exigences relatives à la détection des événements
Reprise après sinistre	Exigences relatives à la reprise après sinistre
Expiration	Exigences relatives à l'expiration des comptes et mots de passe
Installation	Exigences relatives à l'installation des outils et logiciels liés à la sécurité
Registre d'inventaire	Exigences relatives au document qui récapitule les appareils et leurs composants logiciels utilisés dans la Solution d'Automatisation
Fonctionnalité minimale	Exigences relatives à la prise en charge du concept de fonctionnalité minimale (par exemple, la désactivation d'un service inutile ou la suppression d'un compte temporaire qui n'est plus en utilisation). Voir l'IEC 62443-3-3 pour plus d'informations sur la fonctionnalité minimale
Journalisation	Exigences relatives aux journaux d'audit et d'événements
Fichiers de définition de logiciel malveillant	Exigences relatives à l'approbation et l'utilisation de fichiers de définition de logiciel malveillant.
Mécanisme de protection contre les logiciels malveillants	Exigences relatives à l'utilisation de mécanismes de protection contre les logiciels malveillants (logiciel antivirus, logiciel de liste blanche, par exemple).
Temps réseau	Exigences relatives à la distribution et la synchronisation du temps sur le réseau
Qualification des correctifs	Exigences relatives à l'évaluation et l'approbation des correctifs à utiliser dans la Solution d'Automatisation
Réalisation	Exigences relatives à la réalisation d'une capacité pour la Solution d'Automatisation
Génération de rapports	Exigences relatives à la génération de rapports d'événements (des notifications, par exemple)
Génération de réponses	Exigences relatives à la gestion et la génération de réponses aux événements
Processus de restauration	Exigences relatives au processus de restauration de la Solution d'Automatisation après sauvegarde
Restrictions	Exigences relatives aux capacités de restriction/contrainte
Réutilisation	Exigences relatives à la réutilisation des mots de passe
Robustesse	Exigences relatives à l'aptitude de la Solution d'Automatisation et ses composants à résister à des données anormales, des séquences anormales ou à des volumes anormalement élevés de trafic sur le réseau (alarmes et analyses de réseau, par exemple)
Nettoyage	Exigences relatives au nettoyage des appareils et supports portables pour retirer des données sensibles et/ou supprimer des logiciels malveillants
Contact de sécurité	Exigences qui définissent et exigent le rôle de "contact de sécurité"
Responsable de la sécurité	Exigences qui définissent et exigent le rôle de "responsable de la sécurité"

Valeur	Description
Exigences de sécurité – …	Exigences relatives aux exigences de sécurité contenues dans la présente spécification ou définies par le propriétaire d'actif
Données sensibles	Exigences relatives aux données devant faire l'objet d'une protection
Fournisseur de service	Exigences relatives au personnel du fournisseur de service ou à ses capacités
Verrouillage de session	Exigences relatives au verrouillage du clavier et de l'écran des stations de travail
Partagé	Exigences relatives au partage des mots de passe
Sous-traitant	Exigences relatives au personnel ou aux capacités des sous-traitants, consultants ou représentants du fournisseur de service
Description technique	Exigences relatives aux descriptions de certains aspects techniques de la Solution d'Automatisation
Usage	Exigences relatives à l'utilisation ou l'application d'une capacité exigée
Vérification	Exigences relatives à la vérification d'une capacité (par une démonstration ou une inspection visuelle, par exemple)
Identificateurs de réseau sans fil	Exigences relatives aux identificateurs des réseaux sans fil

5.5.6 Colonne Documentation

Cette colonne contient une valeur Oui pour indiquer que l'exigence décrit une capacité exigeant une documentation livrable au propriétaire d'actif. Les exigences dont la valeur est Non peuvent obliger le fournisseur de service à créer et/ou gérer la documentation à l'appui de la capacité exigée, cette documentation n'étant cependant pas considérée comme étant livrable au propriétaire d'actif. Toutefois, dans le cadre d'accords séparés, le propriétaire d'actif peut demander que la documentation soit considérée comme étant livrable.

5.5.7 Description de l'exigence

Cette colonne contient la description textuelle de l'exigence. Elle peut également contenir des notes qui sont des exemples facilitant la compréhension de l'exigence.

Chaque exigence définit une capacité exigée du fournisseur de service. Le fait qu'un propriétaire d'actif exige du fournisseur de service qu'il exécute la capacité ne relève pas du domaine d'application de la présente norme.

L'expression "communément accepté par les communautés de sécurité et d'automatisation industrielle" est utilisée dans ces descriptions d'exigences pour éviter les exigences pour les technologies spécifiques (algorithmes de chiffrement spécifiques, par exemple). Elle est plutôt utilisée pour exiger des instances de concepts spécifiés (le chiffrement, par exemple) communément acceptées et utilisées par les deux communautés. Par exemple, le mécanisme de chiffrement qu'un fournisseur de service utilise pour satisfaire à ce type d'exigence dépend du moment auquel la présente norme est appliquée.

5.5.8 Justification

Cette colonne contient la justification qui décrit le raisonnement sous-tendant chaque exigence (c'est-à-dire l'objet/avantage de la capacité exigée) et donne des lignes directrices supplémentaires pour une meilleure compréhension de chaque exigence. Dans la plupart des descriptions, la terminologie "dispose d'un processus identifiable" est utilisée. Le terme "identifiable" signifie que le fournisseur de service dispose d'un processus qu'il peut utiliser et qu'il peut faire connaître (identifier) au propriétaire d'actif et exécuter pour lui. L'application du modèle de maturité décrit en 4.2 signifie que ce processus peut ne pas encore être formellement documenté (niveau de maturité 1).

Annexe A
(normative)

Exigences de sécurité

Tableau A.1 – Exigences de programme de sécurité

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.01.01	BR	Affectation en personnel pour la Solution	Formation	Exigences de sécurité – IEC 62443-2-4	Non	Le fournisseur de service doit être en mesure de garantir qu'il affecte uniquement son personnel aux activités liées à la Solution d'Automatisation, ledit personnel ayant été informé et respectant les responsabilités, les politiques et les procédures exigées par la présente spécification.	Les capacités spécifiées par cette exigence de base (BR) et ses améliorations d'exigences (RE) sont utilisées pour protéger la Solution d'Automatisation contre les menaces provenant du personnel du fournisseur de service, du personnel sous-traitant et du personnel du consultant qui ne sont pas conscients de leurs responsabilités courantes en matière de sécurité (les meilleures pratiques de sécurité, par exemple). Trop souvent, les failles de sécurité résultent d'une action initiée par le personnel qui sans le savoir viole une meilleure pratique de sécurité (par exemple, enficher une clé USB non autorisée) ou d'un manque d'action appropriée (non mise à jour d'une règle de pare-feu d'un périmètre après suppression d'une station de travail externe). Cela signifie que le fournisseur de service est en mesure de fournir du personnel sensibilisé à la sécurité pour travailler sur la Solution d'Automatisation. Les méthodes d'information du personnel incluent généralement la formation et/ou l'examen de procédures. NOTE 1 Les propriétaires d'actif peuvent demander de valider la formation par écrit. NOTE 2 Les niveaux de maturité 3 et 4 (voir 4.2) sont applicables à l'exécution (respect) des responsabilités, politiques et procédures.
SP.01.01	RE(1)	Affectation en personnel pour la Solution	Formation	Exigences de sécurité – IEC 62443-2-4	Non	Le fournisseur de service doit être en mesure de garantir qu'il affecte uniquement le personnel sous-traitant ou le consultant aux activités liées à la Solution d'Automatisation, ledit personnel ayant été informé et respectant les responsabilités, les politiques et les procédures exigées par la présente spécification.	Cela signifie que le fournisseur de service est en mesure de fournir le personnel sous-traitant, les consultants et les représentants sensibilisés à la sécurité pour travailler sur la Solution d'Automatisation. Voir l'ISO/IEC 27036-3 pour connaître les exigences organisationnelles supplémentaires liées à la chaîne logistique.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.01.02	BR	Affectation en personnel pour la Solution	Formation	Exigences de sécurité – propriétaire d'actif	Non	Le fournisseur de service doit être en mesure de garantir qu'il affecte uniquement son personnel, le personnel du consultant ou le personnel sous-traitant aux activités liées à la Solution d'Automatisation, ledit personnel ayant été informé et respectant les responsabilités, les politiques et les procédures relatives à la sécurité exigées par le propriétaire d'actif	La capacité spécifiée par cette BR réduit le plus possible les menaces pour la Solution d'Automatisation qui pourraient émaner du personnel du fournisseur de service, du personnel sous-traitant et du personnel du consultant qui ne sont pas conscients de leurs responsabilités de sécurité spécifiques à la Solution d'Automatisation (telles que définies par le propriétaire d'actif). Trop souvent, des failles de sécurité proviennent du personnel qui n'est pas au courant des exigences de sécurité définies par le propriétaire d'actif (par exemple mauvais usage ou mauvais partage d'un compte de maintenance). Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir que le personnel chargé de travailler sur la Solution d'Automatisation est compétent et qu'il respecte les exigences de sécurité du propriétaire d'actif. Cela concerne le personnel du fournisseur de service, ainsi que ses sous-traitants, consultants et représentants. Les méthodes d'information du personnel incluent généralement la formation et/ou l'examen de procédures. Voir l'ISO/IEC 27036-3 pour connaître les exigences organisationnelles supplémentaires liées à la chaîne logistique. NOTE 1 Les propriétaires d'actif peuvent exiger de valider la formation par écrit. NOTE 2 Les niveaux de maturité 3 et 4 (voir 4.2) sont applicables à l'exécution (respect) des responsabilités, politiques et procédures.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.01.02	RE(1)	Affectation en personnel pour la Solution	Formation	Exigences de sécurité – propriétaire d'actif	Non	Le fournisseur de service doit être en mesure de garantir qu'il affecte uniquement son personnel, celui du sous-traitant ou du consultant aux activités liées à la Solution d'Automatisation, ledit personnel ayant été informé et se conformant aux processus de Gestion des modifications (MoC) et d'Autorisation de travail (PtW) du propriétaire d'actif pour les modifications concernant les appareils, les stations de travail, les serveurs et les connexions entre eux.	La capacité spécifiée par cette RE réduit le plus possible les menaces pour la Solution d'Automatisation liées au personnel du fournisseur de service ayant un accès non autorisé à la Solution d'Automatisation et apportant des modifications non autorisées à la Solution d'Automatisation. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir que le personnel prévu pour travailler sur la Solution d'Automatisation est compétent et qu'il se conforme aux processus de Gestion des modifications (MoC) et d'Autorisation de travail (PtW) du propriétaire d'actif pour s'assurer que les modifications apportées aux appareils/stations de travail/serveurs sont correctement gérées. NOTE Les niveaux de maturité 3 et 4 (voir 4.2) sont applicables à l'exécution (respect) des responsabilités, politiques et procédures.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.01.03	BR	Affectation en personnel pour la Solution	Formation	Données sensibles	Non	Le fournisseur de service doit être en mesure de garantir qu'il affecte uniquement son personnel aux activités liées à la Solution d'Automatisation, ledit personnel ayant a été informé et se conformant aux politiques, procédures et obligations contractuelles exigées pour protéger la confidentialité des données du propriétaire d'actif.	Les capacités spécifiées par cette BR et ses RE sont utilisées pour protéger la Solution d'Automatisation contre le mauvais traitement des données du propriétaire d'actif permettant ainsi leur divulgation (par exemple, imprimer une procédure et la laisser sans surveillance ou dans un endroit où elle peut être vue par les passants). Cela signifie que le fournisseur de service est capable de fournir du personnel conscient de ses responsabilités pour travailler sur la Solution d'Automatisation, et protéger les données exclusives du propriétaire d'actif contre la divulgation. Il est classique d'utiliser un accord de confidentialité pour définir les termes liés à la protection des données confidentielles, y compris les données à protéger et pour lesquelles existent des exigences particulières de traitement. En outre, cette capacité exige de la part du fournisseur de service de disposer d'un processus identifiable permettant d'informer son personnel quant à l'existence et aux conditions de cet accord de confidentialité. De plus, les propriétaires d'actif peuvent exiger de prouver (par écrit, par exemple) que le personnel a bien été informé de ces responsabilités. Voir l'ISO/IEC 27036-3 pour connaître les exigences organisationnelles supplémentaires liées à la chaîne logistique entre le propriétaire d'actif et le fournisseur de service. NOTE Les niveaux de maturité 3 et 4 (voir 4.2) sont applicables à l'exécution (respect) des responsabilités, politiques et procédures.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.01.03	RE(1)	Affectation en personnel pour la Solution	Formation	Données sensibles	Non	Le fournisseur de service doit être en mesure de garantir qu'il affecte uniquement les sous-traitants, les consultants et les représentants aux activités liées à la Solution d'Automatisation, lesquels ont été informés et se conforment aux politiques et procédures exigées pour protéger la confidentialité des données du propriétaire d'actif.	Cela signifie que le fournisseur de service est capable de garantir que le sous-traitant, le consultant et les représentants affectés au travail sur la Solution d'Automatisation sont conscients de leurs responsabilités pour protéger les données exclusives du propriétaire d'actif contre la divulgation. Il est classique d'utiliser un accord de confidentialité pour définir les termes liés à la protection des données confidentielles, y compris les données à protéger et pour lesquelles existent des exigences particulières de traitement. En outre, cette capacité exige de la part du fournisseur de service de disposer d'un processus identifiable permettant d'informer ces personnels quant à l'existence et aux conditions de cet accord de confidentialité. De plus, les propriétaires d'actif peuvent exiger de prouver (par écrit, par exemple) que le personnel a bien été informé de ces responsabilités. Voir l'ISO/IEC 27036-3 pour connaître les exigences organisationnelles supplémentaires liées à la chaîne logistique entre le propriétaire d'actif et le fournisseur de service. NOTE Les niveaux de maturité 3 et 4 (voir 4.2) sont applicables à l'exécution (respect) des responsabilités, politiques et procédures.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.01.04	BR	Affectation en personnel pour la Solution	Vérifications des antécédents	Fournisseur de service	Non	Le fournisseur de service doit être en mesure de garantir qu'il affecte uniquement son personnel aux activités liées à la Solution d'Automatisation, lequel a subi avec succès des vérifications d'antécédents relatives à la sécurité, dans la mesure autorisée par la loi.	Les capacités spécifiées par cette BR et ses RE sont utilisées pour empêcher que la Solution d'Automatisation soit dotée d'un personnel dont la fiabilité peut être discutable. Bien que la vérification des antécédents ne puisse garantir la fiabilité, elle peut aider à identifier le personnel qui a des problèmes de fiabilité Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de vérifier l'intégrité de son personnel qu'il affecte au travail sur la Solution d'Automatisation. Cette exigence reconnaît également qu'il n'est pas toujours possible de procéder à des vérifications d'antécédents en raison des lois en vigueur. La manière et la fréquence de ces vérifications d'antécédents sont laissées à la discrétion du fournisseur de service. Des exemples de vérifications d'antécédents incluent la vérification d'identité et les demandes de casier judiciaire.
SP.01.04	RE(1)	Affectation en personnel pour la Solution	Vérifications des antécédents	Sous-traitant	Non	Le fournisseur de service doit être en mesure de garantir qu'il affecte uniquement les sous-traitants, consultants et représentants aux activités liées à la Solution d'Automatisation, lesquels ont subi avec succès des vérifications d'antécédents relatives à la sécurité, dans la mesure autorisée par la loi.	Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de vérifier l'intégrité de ses sous-traitants, consultants et représentants qu'il affecte au travail sur la Solution d'Automatisation. Cette exigence reconnaît également qu'il n'est pas toujours possible de procéder à des vérifications d'antécédents en raison des lois en vigueur. La manière et la fréquence de ces vérifications d'antécédents sont laissées à la discrétion du fournisseur de service. Des exemples de vérifications d'antécédents incluent la vérification d'identité et les demandes de casier judiciaire. Voir l'ISO/IEC 27036-3 pour connaître les exigences organisationnelles supplémentaires liées à la chaîne logistique.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.01.05	BR	Affectation en personnel pour la Solution	Affectations de personnel	Contact de sécurité	Non	Le fournisseur de service doit être en mesure d'affecter un contact de sécurité dans son organisation à la Solution d'Automatisation, lequel est responsable et redevable des activités suivantes. 1) Assure la liaison avec le propriétaire d'actif, selon le cas, quant à la conformité du fournisseur de service et de la Solution d'Automatisation aux exigences de la Partie 2-4 exigée par le propriétaire d'actif. 2) Communique le point de vue du fournisseur de service sur la sécurité IACS au personnel du propriétaire d'actif. 3) Vérifie que les offres adressées au propriétaire d'actif satisfont aux exigences de la Partie 2-4 spécifiée, comme exigé par le propriétaire d'actif, ainsi qu'aux exigences de sécurité IACS internes du fournisseur de service. 4) Communique au propriétaire d'actif les écarts ou autres absences de conformité aux exigences de la Partie 2-4 formulées par le propriétaire d'actif. Il s'agit des écarts entre ces exigences et les exigences internes du fournisseur de service.	La capacité spécifiée par cette BR est utilisée pour améliorer la communication en matière de sécurité entre le propriétaire d'actif et le fournisseur de service pour permettre au fournisseur de service de mieux répondre aux besoins de sécurité de la Solution d'Automatisation. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant d'affecter une personne à la Solution d'Automatisation, qui sera chargée de coordonner les questions relatives à la sécurité avec le propriétaire d'actif, comme les écarts par rapport aux exigences de la Partie 2-4 et de la Partie 3-3. La possession d'un contact de sécurité offre au propriétaire d'actif le moyen institutionnel de travailler avec le fournisseur de service pour résoudre les écarts par rapport aux capacités de la Partie 2-4 et les écarts du système de commande utilisé dans la Solution d'Automatisation par rapport aux exigences de la Partie 3-3 (par exemple la façon de fournir des mécanismes de compensation).

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.01.06	BR	Affectation en personnel pour la Solution	Affectations de personnel	Responsable de la sécurité	Non	Le fournisseur de service doit être en mesure d'affecter aux Solutions d'Automatisation des responsables de la sécurité ayant démontré des compétences en matière de cybersécurité IACS.	La capacité spécifiée par cette BR est utilisée pour réduire les erreurs dans la prise de décision et la mise en œuvre en matière de sécurité. Des choix inappropriés ou des insuffisances d'aptitude à mettre convenablement en œuvre les mesures de sécurité peuvent exposer inutilement la Solution d'Automatisation aux menaces et/ou failles de sécurité. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant d'affecter à chaque Solution d'Automatisation du personnel suffisamment qualifié pour prendre en charge les activités liées à la cybersécurité. L'expertise peut inclure une expérience, une formation et des certifications en cybersécurité IACS, les qualifications du personnel en la matière avant le démarrage de l'affectation en personnel devant en général faire l'objet d'un accord entre le fournisseur de service et le propriétaire d'actif. Le terme "ayant démontré" est utilisé pour indiquer que les responsables de la sécurité affectés à la Solution d'Automatisation disposent d'éléments probants de leur expérience.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.01.07	BR	Affectation en personnel pour la Solution	Affectations de personnel	Modification	Non	Le fournisseur de service doit être en mesure d'informer le propriétaire d'actif des changements de son personnel et de celui du sous-traitant ou du consultant ayant accès à la Solution d'Automatisation.	La capacité spécifiée par cette BR est utilisée pour protéger la Solution d'Automatisation contre les menaces posées par le personnel du fournisseur de service, le personnel du sous-traitant et/ou le personnel du consultant qui n'ont plus besoin d'accéder à la Solution d'Automatisation. Une fois avisé des changements du personnel, le propriétaire d'actif peut mettre à jour les autorisations d'accès en conséquence (par exemple, la révocation des badges, la suppression des comptes d'utilisateurs et les listes de contrôle d'accès associées). Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant d'informer le propriétaire d'actif des changements d'affectation de son personnel. L'opportunité de la notification et les changements d'affectation de personnel devant faire l'objet d'une notification sont des éléments classiques convenus entre le fournisseur de service et le propriétaire d'actif. Par exemple, le personnel du fournisseur de service ayant accès à la Solution d'Automatisation grâce à des comptes temporaires peut ne pas être inclus, les comptes temporaires expirant lorsqu'ils deviennent inutiles.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.02.01	BR	Assurance	Composants de la Solution	Vérification	Oui	Le fournisseur de service doit être en mesure de fournir la documentation selon laquelle les composants de la Solution d'Automatisation identifiés par le fournisseur d'actif (par exemple, à l'issue d'une évaluation de sécurité, d'une analyse des menaces et/ou des essais de sécurité) ont une sécurité adéquate pour leur niveau de risque.	La capacité spécifiée par cette BR est utilisée pour donner l'assurance que les composants de la Solution d'Automatisation ont des capacités de sécurité correspondant à leur niveau de risque de sécurité. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de confirmer que les composants de la Solution d'Automatisation fournissent le niveau approprié de moyens de protection en matière de sécurité exigé par le propriétaire d'actif. Les évaluations et certifications de sécurité, les essais et /ou d'autres méthodes peuvent être utilisés pour fournir cette confirmation. L'essai de sécurité se rapporte à l'essai de système ou de composant dont l'objectif principal est de déceler les vulnérabilités et, inversement, de vérifier que les attaques spécifiques sont gérées comme prévu (par exemple, atténuées, vaincues et/ou détournées/mises en quarantaine). Le succès des essais de sécurité ne signifie pas nécessairement que l'élément en essai ne comporte aucune vulnérabilité. Des exemples d'essai de sécurité incluent les essais de pénétration, les essais de distorsion, les essais de robustesse et les analyses de vulnérabilité. Pour les exigences connexes de chaîne logistique, voir l'IEC 62443-4-1, l'IEC 62443-4-2 et l'ISO 27036-3.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.02.02	BR	Assurance	Outils et logiciels de sécurité	Description technique	Oui	Le fournisseur de service doit être en mesure de recommander des outils d'analyse de sécurité (outils d'analyse du réseau, par exemple) à utiliser avec la Solution d'Automatisation, et: 1) de fournir des instructions sur la manière de les utiliser, 2) d'identifier tous les effets néfastes connus sur les performances de la Solution d'Automatisation, 3) de fournir des recommandations quant à la manière d'éviter ces effets néfastes.	Les capacités spécifiées par cette BR et ses RE sont utilisées pour garantir que la Solution d'Automatisation peut être examinée pour les questions relatives à la sécurité à l'aide d'outils approuvés par le propriétaire d'actif. Les questions relatives à la sécurité comprennent la détection d'appareils non autorisés sur le réseau et/ou de ports ouverts non autorisés sur un appareil. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de recommander un ou plusieurs outils d'analyse de sécurité pour la Solution d'Automatisation, de donner des informations relatives à d'éventuels problèmes engendrés par leur utilisation, et des instructions quant à la manière d'éviter ces problèmes. Cette exigence implique directement que le fournisseur de service est tenu d'être conscient des problèmes potentiels que présente un outil qu'il recommande, et de les signaler au propriétaire d'actif avec des recommandations sur la manière de les éviter et sur la manière d'utiliser l'outil efficacement. Ces problèmes potentiels associés à l'utilisation d'un outil peuvent être évités en limitant les options de configuration, en planifiant des essais en temps opportuns ou par d'autres moyens. Par exemple, si un outil d'analyse de réseau est réputé être susceptible de surcharger le réseau, il peut être configuré de manière à limiter son impact sur le trafic du réseau ou le réseau peut être segmenté pour réduire la portée des surcharges.
SP.02.02	RE(1)	Assurance	Outils et logiciels de sécurité	Approbation	Non	Le fournisseur de service doit être en mesure de garantir qu'il obtient l'approbation du propriétaire d'actif avant d'utiliser des outils d'analyse de sécurité (des analyses de réseau, par exemple) sur le site du propriétaire d'actif.	Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de coordonner l'utilisation des outils d'analyse de sécurité dans la Solution d'Automatisation avec le propriétaire d'actif et d'être autorisé à les utiliser. L'exigence de base (BR) de cette amélioration d'exigence (RE) oblige le fournisseur de service à être en mesure d'informer le propriétaire d'actif d'éventuels effets néfastes que ces outils peuvent avoir sur la Solution d'Automatisation.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.02.02	RE(2)	Assurance	Outils et logiciels de sécurité	Détection	Non	Le fournisseur de service doit être en mesure de planifier et d'utiliser des outils d'analyse de sécurité afin de détecter des systèmes ou vulnérabilités non documenté(e)s et/ou non autorisé(e)s dans la Solution d'Automatisation. Cela doit inclure l'aptitude à utiliser ces outils conformément aux procédures normalisées de fonctionnement du propriétaire d'actif.	Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant d'utiliser des outils afin de détecter les appareils non autorisés connectés aux réseaux dans la Solution d'Automatisation, ainsi que d'autres vulnérabilités (les ports ouverts qu'il convient de ne pas ouvrir, par exemple). Cela signifie également que le fournisseur de service dispose d'un processus identifiable permettant de coordonner et de planifier l'utilisation d'outils d'analyse de sécurité afin d'éviter qu'ils n'aient un impact sur le fonctionnement de la Solution d'Automatisation. L'exigence de base (BR) de cette amélioration d'exigence (RE) oblige le fournisseur de service à informer le propriétaire d'actif d'éventuels effets néfastes que ces outils peuvent avoir sur la Solution d'Automatisation. Les fournisseurs de service d'intégration sont encouragés à planifier l'utilisation de ces outils juste avant le transfert (afin de détecter les appareils non autorisés et les ports ouverts, par exemple) alors qu'il convient que les fournisseurs de service de maintenance les utilisent régulièrement en fonction des cycles définis par le propriétaire d'actif. NOTE Le cas échéant, il convient que les analyses de réseau recherchent les appareils sur les segments de réseau filaire et sans fil dans la Solution d'Automatisation.
SP.02.02	RE(3)	Assurance	Outils et logiciels de sécurité	Robustesse	Non	Le fournisseur de service doit être en mesure de garantir que les composants du système de commande utilisés dans la Solution d'Automatisation sont capables de maintenir les fonctions essentielles du système de commande en présence d'analyses de système et/ou de réseau pendant le fonctionnement normal.	Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir que les composants du système de commande de la Solution d'Automatisation, auxquels peuvent accéder les outils d'analyse de réseau, sont capables de résister à ces analyses. Voir l'IEC 62443-3-3 pour les capacités de système liées aux analyses de réseau. Les essais de robustesse servent souvent à prouver cette assurance.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.02.03	BR	Assurance	Lignes directrices de renforcement	Description technique	Oui	Le fournisseur de service doit être en mesure de fournir au propriétaire d'actif la documentation décrivant la manière de renforcer la Solution d'Automatisation.	Les capacités spécifiées par cette BR et son RE sont utilisées pour fournir au propriétaire d'actif des informations sur les mécanismes de sécurité et les paramètres de configuration de la Solution d'Automatisation. Ceci appuie les initiatives du propriétaire d'actif à assurer la gouvernance et des informations détaillées sur la sécurité de la Solution d'Automatisation, y compris l'intégration de la Solution d'Automatisation avec des réseaux et des systèmes d'usine. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de proposer un guide de renforcement de la Solution d'Automatisation (installer/configurer les fonctions de sécurité de la Solution d'Automatisation). Il est nécessaire d'inclure dans ce guide des considérations relatives à l'architecture et à la configuration (la place du pare-feu (architecture) et les règles de pare-feu (configuration), par exemple), ainsi que des considérations relatives à l'installation de nouveaux composants dans la Solution d'Automatisation. En général, le renforcement de la Solution d'Automatisation. se conforme aux recommandations formulées suite à une appréciation du risque réalisée sur la Solution d'Automatisation. (voir SP.03.01.BR et ses RE). NOTE Les guides de renforcement fournis par les fournisseurs du système de commande et d'autres composants utilisés dans la Solution d'Automatisation peuvent être inclus dans ou référencés par le guide de renforcement du fournisseur de service.
SP.02.03	RE(1)	Assurance	Lignes directrices de renforcement	Vérification	Non	Le fournisseur de service doit être en mesure de vérifier que ses lignes directrices et procédures en matière de renforcement de la sécurité sont respectées pendant les activités liées à la Solution d'Automatisation.	Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir que le personnel et leurs sous-traitants/consultants/représentants suivent les procédures de renforcement exigées dans SP.02.03.BR. Des listes de contrôle sont souvent utilisées à cet effet.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.03.01	BR	Architecture	Appréciation du risque	Réalisation	Non	Le fournisseur de service doit être en mesure de mener une appréciation du risque de sécurité de la Solution d'Automatisation ou contribuer (participer) à l'appréciation du risque de sécurité effectuée par le propriétaire d'actif ou son agent. NOTE 1 Le propriétaire d'actif peut en outre exiger du fournisseur de service qu'il documente son évaluation. La colonne "Doc?" est définie sur "Non" parce qu'il s'agit d'une exigence relative à la capacité de réaliser l'évaluation et non d'une exigence de fournir de la documentation.	Les capacités spécifiées par cette BR et ses RE sont utilisées pour garantir que le fournisseur de service est en mesure d'identifier et d'analyser les risques pour prendre en charge l'identification et la résolution des risques de sécurité pour la Solution d'Automatisation. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de réaliser ou de participer à une appréciation du risque. Dans certains cas, le propriétaire d'actif exige du fournisseur de service qu'il mène l'évaluation, alors que dans d'autres cas, il exige qu'il joue un rôle actif dans l'évaluation menée par le propriétaire d'actif ou par un tiers sous la direction du propriétaire d'actif. Dans un rôle actif, il peut être demandé au fournisseur de service de renseigner de manière détaillée sur la Solution d'Automatisation et ses composants, de donner des informations relatives aux menaces et/ou vulnérabilités ou d'aider à une évaluation à laquelle le propriétaire d'actif a largement participé/contribué. Pour les lignes directrices relatives à la réalisation des appréciations des risques, voir l'IEC 62443-2-1 et l'IEC 62443-3-2. NOTE 2 Les risques de sécurité peuvent être évalués à tous les stades de la conception et de la mise en œuvre de la Solution d'Automatisation, afin d'identifier et de gérer ces risques. Cependant l'évaluation est souvent effectuée avant la conception de la Solution d'Automatisation pour servir de base aux décisions de conception en matière de sécurité, et elle est souvent répétée pour s'assurer que les risques de sécurité sont actualisés. NOTE 3 L'appréciation du risque réalisée au moment de la mise en service permet au propriétaire d'actif de se repérer en fonction du système de sécurité obtenu ou conforme à l'exécution. NOTE 4 Le résultat de l'appréciation du risque de sécurité est un élément contractuel entre le fournisseur de service et le propriétaire d'actif.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.03.01	RE(1)	Architecture	Appréciation du risque	Génération de rapports	Non	Le fournisseur de service doit informer le propriétaire d'actif des résultats des appréciations des risques de sécurité qu'il réalise sur la Solution d'Automatisation, y compris les mécanismes et procédures d'atténuation des risques.	Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant d'examiner les appréciations des risques de la Solution d'Automatisation qu'il a réalisées, et d'informer le propriétaire d'actif des problèmes de sécurité qui ont été détectés, y compris les recommandations en matière de mécanismes/procédures de sécurité permettant de les résoudre
SP.03.01	RE(2)	Architecture	Appréciation du risque	Vérification	Non	Le fournisseur de service doit être en mesure de vérifier que les revues d'architecture de sécurité et/ou l'appréciation du risque de sécurité et/ou l'analyse des menaces du système de commande utilisé dans la Solution d'Automatisation ont été menées par un tiers.	Cela signifie que le fournisseur de service peut prouver que la sécurité du système de commande utilisé dans la Solution d'Automatisation a été examinée par un tiers. En règle générale, l'examen est réalisé sur le produit de système de commande sous la direction du fournisseur du système de commande.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.03.02	BR	Architecture	Conception du réseau	Connectivité	Non	Le fournisseur de service doit être en mesure de garantir que l'architecture de segmentation de réseau physique utilisée dans la Solution d'Automatisation, y compris son utilisation d'appareils de sécurité du réseau ou de mécanismes équivalents, est mise en œuvre conformément à la conception de la Solution d'Automatisation approuvée par le propriétaire d'actif.	Les capacités spécifiées par cette BR et ses RE sont utilisées pour garantir l'utilisation de contrôles d'accès entre les segments de réseau au sein de la Solution d'Automatisation et entre la Solution d'Automatisation et les réseaux externes/ liaisons de communication. Les contrôles d'accès protègent les segments de réseau en limitant les flux de trafic entre eux. Les restrictions sont généralement définies par des règles qui mettent sur une liste blanche et/ou noire le trafic basé sur un certain nombre de facteurs, dont les adresses de source, les adresses de destination et le contenu (l'inspection approfondie des paquets, par exemple). Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir que les réseaux de la Solution d'Automatisation ont été segmentés comme indiqué et conformément à la validation du propriétaire d'actif. Il convient de choisir l'emplacement des points de segmentation de réseau et leurs appareils de sécurité de réseau correspondants en fonction de l'appréciation du risque (voir l'IEC 62443-3-2) et des exigences de la présente norme (IEC 62443-2-4). Au fur et à mesure de l'avancée de la mise en œuvre, cela signifie également que le fournisseur de service dispose d'un processus identifiable permettant de garantir la mise à jour des documents de conception de sorte qu'ils reflètent exactement l'architecture de la Solution d'Automatisation (voir SP.06.01.BR).

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.03.02	RE(1)	Architecture	Conception du réseau	Connectivité	Non	Le fournisseur de service doit être en mesure d'identifier et de documenter les segments de réseau de la Solution d'Automatisation et de leurs interfaces avec d'autres segments, y compris les réseaux externes et, pour chaque interface, indiquer si elle est digne de confiance ou pas.	Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant d'identifier tous les segments de réseau de la Solution d'Automatisation, la manière dont ils sont interconnectés, lesquels d'entre eux assurent un accès externe à la Solution d'Automatisation, et d'indiquer chaque point de connexion (interface vers/depuis un segment) comme étant digne de confiance ou pas. Les interfaces qui ne sont pas dignes de confiance sont celles qui autorisent des connexions à d'autres segments/systèmes à partir d'appareils qui ne sont pas dignes de confiance. Les appréciations des risques, telles qu'elles sont décrites dans l'IEC 62443-3-2, peuvent permettre de déterminer le caractère digne de confiance et l'utilisation de zones visant à établir des limites de confiance

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.03.02	RE(2)	Architecture	Conception du réseau	Connectivité	Non	Le fournisseur de service doit être en mesure de garantir que les interfaces de la Solution d'Automatisation qui ont été identifiées comme n'étant pas dignes de confiance sont protégées par des appareils de sécurité de réseau ou des mécanismes équivalents, avec des règles de sécurité documentées et maintenues. Les éléments suivants doivent au moins être protégés: 1) Interfaces externes 2) Interfaces Niveau 2/Niveau 3 (voir NOTE 2 ci-dessous) 3) Interfaces entre le système de commande de processus de base (BPCS) et le système équipé pour la sécurité (SIS) 4) Interfaces de connexion des réseaux BPCS filaires et sans fil 5) Interfaces de connexion du BPCS aux magasins de données (historisations d'entreprise, par exemple) NOTE 1 Pour certains, la responsabilité de gérer les règles de pare-feu et les transferts de documentation au propriétaire d'actif avant ou au moment de la rotation de la Solution d'Automatisation. Dans ce cas, le rôle du fournisseur de service peut être, comme peut l'exiger le propriétaire d'actif, uniquement de vérifier que les règles de pare-feu sont exactes et à jour. NOTE 2 En fonction de la Solution d'Automatisation, les interfaces Niveau 2/Niveau 3 peuvent constituer une interface ''externe''.	Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de protéger la Solution d'Automatisation contre l'accès externe et de contrôler l'accès de Niveau 2 à partir du Niveau 3 (par exemple, à travers l'utilisation de pare-feu et des règles de pare-feu). Avec la Solution d'Automatisation, cela signifie également que le fournisseur de service dispose d'un processus identifiable permettant de protéger les interfaces BPCS à l'aide d'appareils de sécurité de réseau ou de mécanismes équivalents, et de donner les informations nécessaires à la création de règles de sécurité utilisées pour autoriser/refuser l'accès aux ports et applications BPCS. Si le fournisseur de service fournit ou est responsable de l'appareil de sécurité de réseau ou du mécanisme équivalent, alors il s'agit d'être capable de configurer l'appareil/mécanisme de sécurité de réseau en fonction des besoins. Les appréciations des risques (voir l'IEC 62443-3-2) peuvent permettre de déterminer les interfaces devant faire l'objet d'une protection.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.03.03	BR	Architecture	Composants de la Solution	Vulnérabilités	Non	Le fournisseur de service doit être en mesure de traiter les vulnérabilités qui affectent la Solution d'Automatisation, y compris ses politiques et procédures connexes. Ces capacités doivent concerner: 1) le traitement des vulnérabilités nouvellement découvertes dans la Solution d'Automatisation ou dans ses politiques et procédures connexes dont le fournisseur de service est responsable, et 2) le traitement des vulnérabilités rendues publiques qui affectent la Solution d'Automatisation.	Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant d'évaluer, de générer des rapports et d'éliminer les vulnérabilités (par exemple, recommander un plan d'atténuation, élaboration de plans de correction) liées aux composants de la Solution d'Automatisation dont il est responsable. En règle générale, le processus d'identification des vulnérabilités inclut l'analyse et la corrélation des événements (voir SP.08.01 BR), l'appréciation du risque (voir SP.03.01 BR et ses RE), les analyses de réseau et d'autres méthodes automatisées (voir SP.02.02 BR et ses RE) et l'assurance. Les correctifs logiciels résultant de l'élimination des vulnérabilités sont considérés comme étant des correctifs de sécurité.
SP.03.03	RE(1)	Architecture	Conception du réseau	Vulnérabilités	Oui	Le fournisseur de service doit être en mesure de fournir la documentation au propriétaire d'actif, décrivant la manière de limiter les faiblesses de sécurité inhérentes à la conception et/ou la mise en œuvre des protocoles de communication utilisés dans la Solution d'Automatisation, lesquelles sont connues avant les activités d'intégration ou de maintenance de la Solution d'Automatisation.	La capacité spécifiée par cette BR est utilisée pour garantir que des mécanismes de compensation sont utilisés pour corriger les faiblesses contenues dans les communications de la Solution d'Automatisation. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de signaler au propriétaire d'actif les faiblesses de communication dans la Solution d'Automatisation et la manière de les limiter. Par exemple, si la Solution d'Automatisation utilise des protocoles non chiffrés pour le transfert de données sensibles, il convient que le fournisseur de service recommande des mesures de sécurité, telles que des commutateurs verrouillables et une sécurité physique pour les liaisons de communication, afin de protéger la transmission des données NOTE Le propriétaire d'actif peut aussi exiger du fournisseur de service, dans le cadre de son contrat de prestation de services avec le fournisseur de service ou d'un autre contrat de prestation de services, qu'il l'informe de la détection de faiblesses/atténuations supplémentaires à l'issue du terme normal des activités d'intégration ou de maintenance.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.03.04	BR	Architecture	Conception du réseau	Temps réseau	Non	Le fournisseur de service doit être en mesure de garantir que la distribution en fonction du temps/synchronisation pour la Solution d'Automatisation est assurée à partir d'une source sûre et exacte qui utilise un protocole communément accepté par les communautés de sécurité et d'automatisation industrielle.	La capacité spécifiée par cette BR est utilisée pour garantir que les horodatages sont utilisés dans la Solution d'Automatisation et qu'ils sont générés et distribués par une source fiable. Les horodatages sont utilisés dans des activités d'investigation numérique lors de l'examen des journaux d'événements. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant d'intégrer une source de synchronisation de réseau dans la Solution d'Automatisation. L'aptitude à fournir la source de synchronisation n'entre pas dans le domaine d'application de cette exigence. Toutefois, que le fournisseur de service apporte la source de synchronisation ou pas, son intégration dans la Solution 'Automatisation relève de sa responsabilité. Le protocole IEEE 1588-2008/IEC 61588:2009 est un exemple de protocole de source de synchronisation communément accepté.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.03.05	BR	Architecture	Appareils – Tous	Fonctionnalité minimale	Non	Le fournisseur de service doit être en mesure de garantir que seules les fonctions logicielles et matérielles exigées par la Solution d'Automatisation ou approuvées par le propriétaire d'actif sont activées dans la Solution d'Automatisation. Ceci inclut de garantir au moins que: 1) les applications et services logiciels inutiles (par exemple, le courrier électronique, les applications de bureau, les jeux) et leurs points d'accès de communication connexes (par exemple, les ports TCP/UDP), les appareils USB (par exemple, le stockage de masse, les communications Bluetooth et les communications sans fil sont désactivés et/ou retirés, sauf si la Solution d'Automatisation l'exige. 2) les adresses réseau utilisées sont autorisées, 3) l'accès physique et logique aux ports de diagnostic et de configuration est protégé contre les accès et les utilisations non autorisés.	Les capacités spécifiées par cette BR et ses RE sont utilisées pour limiter l'accès à la Solution d'Automatisation par la suppression/désactivation des fonctions inutiles et la prévention de l'accès non autorisé aux différents types d'interfaces de la Solution d'Automatisation (par exemple appareil de réseau et ports de configuration/diagnostic). Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de réduire la surface d'attaque de la Solution d'Automatisation, de limiter l'accès aux interfaces/ports (ayant été énumérés) pour les utilisateurs autorisés et de maintenir l'état renforcé de la Solution d'Automatisation. Ce processus peut inclure l'utilisation des outils de sécurité de réseau décrits dans SP.02.02 BR et ses améliorations d'exigences. La limitation des applications logicielles et de leurs points d'accès de communication connexes, des appareils USB tels que les appareils de stockage de masse et des capacités de communication sans fil à ce qui est uniquement nécessaire pour exécuter les fonctions d'un appareil utilisé à la fois dans les opérations normales et d'urgence permet de réduire le nombre de voies d'accès dans l'appareil en cas d'attaque. L'identification des points d'accès inutiles et/ou non autorisés (en utilisant des outils d'analyse de réseau, par exemple) est une technique qui peut être utilisée pour déceler des programmes logiciels inutiles.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
						4) les ports non utilisés sur les appareils de réseau (les commutateurs et routeurs, par exemple) sont configurés de manière à empêcher tout accès non autorisé à l'infrastructure de réseau de la Solution d'Automatisation. 5) les processus de maintenance maintiennent le renforcement de la Solution d'Automatisation pendant toute sa durée de vie.	L'identification des adresses réseau non autorisées, par exemple à l'aide des analyses de réseau décrites dans SP.02.02 RE(2), et leur retrait (par déconnexion des appareils auxquels elles sont attribuées, par exemple) limite la source d'attaques actives et passives. Le contrôle des accès aux ports de configuration physiques des appareils (les ports série, par exemple) a pour objet d'éviter ou de réduire le risque de modifications de la configuration de réseau (appareils de réseau) ou de fonctionnement d'autres appareils sans autorisation. Les différentes méthodes de contrôle d'accès incluent l'installation d'un appareil dans une armoire verrouillée, permettant de verrouiller physiquement le port de configuration ou la désactivation du port en cas d'utilisation non autorisée (par un verrou logiciel, par exemple). Le verrouillage des ports de l'appareil de réseau (commutateurs et routeurs) réduit la possibilité de connexion d'un appareil non autorisé au réseau et d'attaques ou de reniflage du réseau. Les produits de système de commande peuvent déjà avoir supprimé des capacités qu'ils n'ont pas utilisées avant ou lors de l'installation, imposant ainsi au fournisseur de service qu'il garantisse qu'elles sont ajoutées/activées seulement si elles sont exigées et approuvées par le propriétaire d'actif. Les processus de maintenance offrent la possibilité de réinitialiser ou reconfigurer des composants de la Solution d'Automatisation déjà renforcés afin de faire disparaître certains aspects du renforcement. Le contrôle de ces processus réduit cette possibilité.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.03.05	RE(1)	Architecture	Appareils – Tous	Fonctionnalité minimale	Non	Les lignes directrices et procédures de renforcement proposées par le fournisseur de service doivent garantir que seuls les certificats numériques nécessaires, autorisés et documentés pour les autorités de certification (CA) sont installés	Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de déterminer les certificats CA qui sont installés et de retirer ceux qui ne sont pas utilisés/autorisés. En règle générale, l'installation et les mises à niveau du système d'exploitation génèrent un ensemble générique de certificats CA à installer, même s'ils ne sont pas exigés pour la Solution d'Automatisation. La limitation des certificats CA à installer uniquement à ceux qui sont nécessaires empêche l'authentification des applications indésirables ou inutiles.
SP.03.06	BR	Architecture	Appareils – Stations de travail	Verrouillage de session	Non	Le fournisseur de service doit être en mesure de prendre en charge l'utilisation du verrouillage de session des stations de travail de la Solution d'Automatisation, comme l'exige le propriétaire d'actif. Cette exigence s'applique uniquement aux stations de travail dont est responsable le fournisseur de service. Le verrouillage de session: 1) empêche la visualisation des informations affichées sur le périphérique d'affichage de l'utilisateur connecté, et 2) verrouille le périphérique d'entrée de l'utilisateur (le clavier ou la souris, par exemple) tant qu'il n'est pas déverrouillé par l'utilisateur de la session ou par un administrateur. NOTE Le verrouillage du périphérique d'entrée de l'utilisateur signifie que l'utilisateur de la station de travail n'est pas en mesure d'utiliser le clavier, sauf pour le déverrouiller.	La capacité spécifiée par cette BR est utilisée pour garantir que des stations de travail peuvent être verrouillées pour empêcher la divulgation d'informations sur le périphérique d'affichage de l'utilisateur (l'écran, par exemple) et l'usage du périphérique d'entrée de l'utilisateur (le clavier ou la souris, par exemple). Cela signifie que le fournisseur de service dispose d'un processus identifiable de verrouillage automatique de l'écran des stations de travail, comme l'exige le propriétaire d'actif. Avec le verrouillage automatique de l'écran, l'écran de la station de travail n'affiche plus les données et empêche la saisie des données tant que l'utilisateur connecté autorisé ne le déverrouille pas, en général en saisissant de nouveau le mot de passe. Les stations de travail dont l'écran est à verrouiller automatiquement sont définies par les exigences de sécurité sur site, qui sont souvent le résultat d'une appréciation du risque (voir l'IEC 62443-3-2). Par exemple, les stations de travail utilisées pour gérer les appareils de réseau et les réseaux sans fil sont en principe laissées sans surveillance dans des endroits accessibles, et exigent donc d'activer le verrouillage de session automatique. Cette exigence s'applique uniquement aux stations de travail dont est responsable le fournisseur de service.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.03.07	BR	Architecture	Appareils – Stations de travail	Contrôle d'accès	Non	Le fournisseur de service doit être en mesure de garantir que les stations de travail filaires et sans fil, y compris les unités portatives, utilisées pour la maintenance et l'ingénierie des appareils de commande/d'instrumentation filaires et sans fil ne contournent pas: 1) les contrôles d'accès de la Solution d'Automatisation pour ces appareils, 2) les systèmes de protection du réseau (les appareils de sécurité de réseau, par exemple) à la limite de la Solution d'Automatisation au Niveau 3. NOTE 1 L'accès direct à ces appareils par des unités portatives qui contournent les contrôles d'accès de la Solution d'Automatisation est interdit NOTE 2 L'accès direct par une unité portative à un appareil sans fil de Niveau 3 qui contourne l'appareil de sécurité de réseau de Niveau 2/3 est interdit.	Les capacités spécifiées par cette BR et ses RE sont utilisées pour garantir que les contrôles d'accès de la Solution d'Automatisation (y compris les mécanismes d'authentification) sont toujours utilisés pour empêcher tout accès non autorisé aux appareils de terrain de la Solution d'Automatisation à partir des stations de travail/unités portatives. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir l'absence de voies directes entre les stations de travail/unités portatives et les appareils de commande /d'instrumentation qui contournent les contrôles d'accès du système de commande. Cette hypothèse part du principe que les contrôles d'accès à ces appareils par des ingénieurs et des opérateurs sont intégrés au système de commande. Toutefois, la maintenance ou l'ingénierie peut être assurée à l'aide d'unités portatives ou d'autres stations de travail qui ne sont pas totalement intégrées au système de commande, ce qui permet de garantir qu'elles ne peuvent pas directement se connecter aux appareils de commande/d'instrumentation en contournant les contrôles d'accès du système de commande.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.03.07	RE(1)	Architecture	Appareils – Stations de travail	Contrôle d'accès	Non	Le fournisseur de service doit être en mesure de prendre en charge l'utilisation de l'authentification à plusieurs facteurs pour les stations de travail de la Solution d'Automatisation comme l'exige le propriétaire d'actif. Cette exigence s'applique uniquement aux stations de travail dont est responsable le fournisseur de service.	Cela signifie que le fournisseur de service dispose d'un processus identifiable d'authentification à plusieurs facteurs dans les stations de travail, comme l'exige le propriétaire d'actif. Cette prise en charge peut inclure l'aptitude à fournir le matériel nécessaire et/ou à configurer les stations de travail pour appliquer l'authentification à plusieurs facteurs. Dans la pratique, le type et le niveau d'authentification utilisés pour les stations de travail sont définis par les exigences de sécurité sur site, qui sont souvent le résultat d'une appréciation du risque (voir l'IEC 62443-3-2). En général, l'authentification à plusieurs facteurs est utilisée pour les stations de travail accessibles par le personnel non autorisé de la Solution d'Automatisation (les stations de travail se trouvant en principe dans des espaces laissés sans surveillance et/ou sans contrôle, par exemple). Cette exigence s'applique uniquement aux stations de travail dont est responsable le fournisseur de service. L'authentification à plusieurs facteurs inclut au moins deux des éléments ci-dessous: 1) un élément connu de l'utilisateur (un mot de passe, par exemple), 2) un élément que possède l'utilisateur (un jeton physique), comme une carte à puce, par exemple, 3) un élément inhérent à l'utilisateur (une analyse rétinienne, par exemple), 4) l'endroit où se trouve l'utilisateur

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.03.08	BR	Architecture	Appareils – Réseau	Fonctionnalité minimale	Non	Le fournisseur de service doit être en mesure de garantir que le droit d'accès minimal est utilisé pour l'administration des appareils de réseau dont le fournisseur de service est responsable.	Cette BR et ses RE reconnaissent que les appareils de réseau sont critiques pour la Solution d'Automatisation, et en conséquence, font souvent l'objet d'attaques. Par conséquent, cette BR et ses RE sont définies pour garantir que les différentes facettes de l'administration des appareils de réseau sont protégées. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant d'appliquer le concept de droit d'accès minimal à l'administration des appareils de réseau. Le droit d'accès minimal pour les opérations d'administration signifie que l'accès est accordé uniquement aux ressources (les répertoires et fichiers, par exemple) nécessaires, les droits d'accès au système d'exploitation étant restreints à ceux qui sont nécessaires uniquement.
SP.03.08	RE(1)	Architecture	Appareils – Réseau	Contrôle d'accès	Non	Le fournisseur de service doit être en mesure de garantir que les contrôles d'accès utilisés pour l'administration des appareils de réseau et des réseaux sans fil incluent des contrôles d'accès basés sur le rôle. NOTE En principe, les appareils de réseau sont uniquement accessibles par les administrateurs. Par conséquent, il est nécessaire de définir un seul rôle pour ces appareils. Toutefois, si les procédures de fonctionnement du propriétaire d'actif permettent aux administrateurs et à d'autres personnes d'accéder aux appareils de réseau, plusieurs rôles peuvent être définis.	Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de configurer les appareils de réseau pour utiliser les contrôles d'accès basés sur le rôle. La définition de rôles distincts permet de définir des listes de contrôle d'accès séparées pour chaque rôle, et donc de prendre en charge le concept de droit d'accès minimal. En principe, les appareils de réseau sont accessibles uniquement par les administrateurs. Un seul rôle nécessite donc d'être défini, et la liste de contrôle d'accès établie en conséquence. Toutefois, si les procédures de fonctionnement du propriétaire d'actif prévoient différents niveaux d'administration de l'appareil de réseau, plusieurs rôles nécessitent d'être définis. Ces rôles sont donc attribués aux utilisateurs capables d'administrer des appareils de réseau. Voir l'IEC 62351-8 pour de plus amples informations sur les contrôles d'accès basés sur le rôle.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.03.08	RE(2)	Architecture	Appareils – Réseau	Cryptographie	Non	Le fournisseur de service doit être en mesure de garantir l'utilisation du chiffrement pour protéger les données en transit ou pas, qui sont utilisées pour l'administration des appareils de réseau (par exemple, mots de passe, données de configuration) et identifiées comme étant des données devant faire l'objet d'une protection (voir SP.03.10 BR et ses RE). NOTE Voir SP.03.10 RE(3) pour les exigences cryptographiques.	Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir que les données utilisées pour l'administration de l'appareil de réseau, qui sont considérées comme des données sensibles comme spécifié dans SP.03.10 BR et ses RE, sont protégées par chiffrement dans l'appareil et sur les liaisons de communication Le chiffrement utilisé sur les liaisons de communication peut être assuré au niveau de la couche de réseau, sur la connexion de la couche de transport ou au niveau du message pour protéger les données ''sur le fil''. L'utilisation du chiffrement dans l'appareil de réseau permet d'empêcher que la configuration fasse l'objet d'attaques de la part de logiciels malveillants dans l'appareil (suite à un piratage informatique, par exemple). Il convient d'envisager l'utilisation des mécanismes de chiffrement (AES_GCM, par exemple) qui assurent la protection de l'intégrité.
SP.03.08	RE(3)	Architecture	Appareils – Réseau	Contrôle d'accès	Non	Le fournisseur de service doit être en mesure de garantir que les contrôles d'accès utilisés pour l'administration des appareils de réseau incluent l'authentification mutuelle	Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de configurer les appareils de réseau pour utiliser l'authentification mutuelle. L'authentification mutuelle permet de valider l'identité de l'utilisateur et de l'appareil de réseau. Elle offre la possibilité à l'appareil de réseau de déterminer si l'utilisateur est autorisé à accéder à l'appareil, et à l'utilisateur de s'assurer que l'appareil est bien celui qu'il prétend être et que son adresse IP n'a pas été usurpée. L'identification forte, le mot de passe utilisateur/certificat de l'appareil et Kerberos (RFC 1510) sont des exemples de techniques utilisées pour assurer l'authentification mutuelle.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.03.09	BR	Architecture	Protection des données	Communications	Non	Le fournisseur de service doit être en mesure de garantir que la Solution d'Automatisation est configurée pour vérifier que toutes les actions de contrôle et les flux de données dans la Solution d'Automatisation (par exemple, entre les stations de travail et les contrôleurs), y compris les changements de configuration, sont: 1) valides, 2) initiés ou approuvés par un utilisateur autorisé, et 3) transférés sur une connexion et dans une direction approuvées.	La capacité spécifiée par cette BR est utilisée pour garantir que des commandes manuelles et/ou automatiques sont en place pour empêcher les appareils de la Solution d'Automatisation, tels que les contrôleurs, d'exécuter des commandes non valides et/ou non autorisées. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir que toutes les commandes (écritures sur des valeurs de consigne, commandes de configuration, par exemple) envoyées aux appareils de la Solution d'Automatisation (à partir des stations de travail, par exemple) sont valides (dans les limites autorisées), sont autorisées par l'utilisateur doté des droits d'accès appropriés et sont transférées vers l'appareil qui exécute la commande (le contrôleur, par exemple) sur une connexion conçue/autorisée à cet effet (une connexion entre une console de l'opérateur et un contrôleur, par exemple). Le deuxième point de l'exigence a pour objet de s'assurer que les commandes peuvent uniquement être demandées par les utilisateurs autorisés (des opérateurs, par exemple), que l'entité qui reçoit et qui exécute la commande connaît les connexions qui sont autorisées pour recevoir des commandes et que la validité de la commande est vérifiée. En règle générale, la validité dépend de la valeur et de l'état. Par exemple, un opérateur n'est pas autorisé à écrire un point de consigne sans placer la boucle dans une commande manuelle.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
							Cette exigence implique également de la part du fournisseur de service de disposer d'un processus identifiable permettant de garantir que les flux de données sont réalisés sur une connexion autorisée et que les données sont transférées dans la direction autorisée. Cette partie de l'exigence a pour objet de s'assurer que le flux de données, y compris la direction, est autorisé et a lieu sur des connexions autorisées. Par exemple, si une modification dynamique (pas une modification de configuration) d'un point de consigne est initiée par une entité qui n'est pas explicitement autorisée à apporter cette modification (une application de commande avancée, par exemple), le système informe l'opérateur de la modification et il faut que l'opérateur l'approuve avant sa prise d'effet. Si l'opérateur ne l'approuve pas, le point de consigne n'est pas modifié. NOTE 1 Cette exigence s'applique généralement aux commandes émises par les stations de travail et envoyées aux contrôleurs, et non les commandes envoyées par les contrôleurs aux appareils de Niveau 1. NOTE 2 L'autorisation des connexions peut être donnée de façon automatique par le système de commande et /ou au moyen d'une configuration appropriée par le fournisseur de service (configuration des adresses /ports réseau autorisés à envoyer des commandes) NOTE 3 Les appréciations des risques (voir IEC 62443-3-2) peuvent permettre de déterminer les connexions qui sont autorisées à réaliser des actions de contrôle. Si l'appréciation du risque le justifie, des capacités de système de "double approbation" (voir l'IEC 62443-3-3) peuvent être utilisées pour prendre en charge cette exigence. La double approbation se rapporte à un système dans lequel des actions sont soumises à l'approbation par deux personnes, ce qui peut avoir de sérieux impacts sur l'IACS.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
							NOTE 4 Le terme "initié ou approuvé par" signifie, par exemple, que la Solution d'Automatisation peut empêcher des opérateurs distants de modifier les points de consigne sans l'approbation de l'opérateur local par l'intermédiaire de la connexion autorisée. La mise en œuvre dépend de la Solution d'Automatisation.
SP.03.10	BR	Architecture	Protection des données	Données sensibles	Oui	Le fournisseur de service doit être en mesure de garantir que les points de stockage de données et les flux de données dans la Solution d'Automatisation qui nécessitent de faire l'objet d'une protection, tel qu'il a été défini ou approuvé par le propriétaire d'actif, sont documentés, y compris les exigences de sécurité pour leur protection (confidentialité, intégrité, par exemple).	Les capacités spécifiées par cette BR et ses RE sont utilisées pour garantir que les données stockées et/ou transférées dans la Solution d'Automatisation qui nécessitent de faire l'objet d'une protection sont protégées de façon adéquate et documentées. En règle générale, le propriétaire d'actif et le fournisseur de service collaborent pour identifier les données du système de commande qui nécessitent d'être protégées (les mots de passe, les certificats, les clés, par exemple) et d'autres données jugées dignes de protection par le propriétaire d'actif (les procédures, par exemple). Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant d'identifier les données dans la Solution d'Automatisation (qu'elles soient en transit ou pas) qui nécessitent d'être protégées, ainsi que le type de protection exigé. La définition des données à protéger contient souvent des critères spécifiques au site, qu'il convient, par conséquent, que le propriétaire d'actif fournisse ou au moins approuve. Les données qui ne transitent pas peuvent être placées dans une mémoire ou dans un appareil de stockage, les données en transit étant celles qui sont transférées d'une entité à une autre (flux de données).

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
							Les types de données à protéger sont par exemple (cette liste n'est pas exhaustive): 1) les informations juridiques ou règlementaires, 2) les données confidentielles du propriétaire d'actif, y compris les données propriétaires (les procédures, par exemple) et les données identifiées dans les accords de confidentialité ou autres documents contractuels, 3) les données de configuration et de fonctionnement (commandes et paramètres, par exemple), 4) les données système, telles que les éléments de chiffrement (clés et certificats, par exemple), les listes de contrôle d'accès, les mots de passe, les données de l'appareil de réseau 5) les journaux d'audit et d'événement, 6) les données de sauvegarde, 7) les données historiques, 8) les magasins de données.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.03.10	RE(1)	Architecture	Protection des données	Données sensibles	Non	Le fournisseur de service doit être en mesure de garantir que les données de la Solution d'Automatisation devant être protégées, comme indiqué dans SP.03.10 BR, le sont contre toute divulgation ou modification non autorisée, qu'elles soient en transit ou pas.	Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir que, suite à l'identification des données sensibles dans une Solution d'Automatisation, des améliorations nécessaires sont apportées à la Solution d'Automatisation pour protéger ces données. Des appréciations des risques (voir l'IEC 62443-3-2) réalisées tôt dans le processus sont souvent utilisées pour l'identification des données devant être protégées. En règle générale, les mécanismes de protection sont les suivants 1) mécanismes de protection contre les vidages de mémoire et les reniflages de réseau non autorisés, 2) mécanismes de chiffrement, y compris: a) les clés de chiffrement, b) les infrastructures de sécurité à clé publique, c) les signatures numériques, d) le transport des données et le chiffrement de message, e) le chiffrement de base de données.
SP.03.10	RE(2)	Architecture	Protection des données	Rétention de données / d'événements	Oui	Le fournisseur de service doit être en mesure de fournir au propriétaire d'actif la documentation décrivant les capacités de rétention fournies par la Solution d'Automatisation pour le stockage/l'archivage des données sensibles. Cette documentation inclut les capacités, les fonctions d'élagage et de purge, les délais de rétention, etc.	Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de documenter la manière dont la Solution d'Automatisation stocke/archive les données sensibles (les données historiques et les événements, par exemple). Il peut s'agir de capacités internes de la Solution d'Automatisation ou de celles devant être exportées dans une archive d'historique. Les données historiques et les événements peuvent être utilisés dans le cadre d'investigations numériques et lors d'analyse et de la corrélation des événements.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.03.10	RE(3)	Architecture	Protection des données	Cryptographie	Non	Le fournisseur de service doit être en mesure de garantir que les mécanismes de chiffrement utilisés dans la Solution d'Automatisation, y compris les algorithmes et la gestion / distribution / protection de clé, sont communément acceptés par les communautés de sécurité et d'automatisation industrielle.	Cela signifie que le fournisseur de service est en mesure de garantir que les composants de la Solution d'Automatisation qu'il fournit utilisent la technologie de chiffrement en cours, généralement acceptée dans les IACS
SP.03.10	RE(4)	Architecture	Protection des données	Nettoyage	Non	Le fournisseur de service doit être en mesure de garantir que, lors du retrait d'un composant de la Solution d'Automatisation, toutes les données du composant devant être protégées (voir SP 03.10 BR) sont définitivement détruites/supprimées.	La capacité spécifiée par cette BR est utilisée pour empêcher les données sensibles dans un composant/appareil qui a été retiré de la Solution d'Automatisation d'être par la suite divulguées à quiconque qui peut avoir accès au composant retiré. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir que les données confidentielles ou sensibles des appareils retirés de la Solution d'Automatisation sont nettoyées. En règle générale, il suffit de détruire la mémoire ou de la nettoyer un certain nombre de fois pour supprimer les données résiduelles. Le nombre de nettoyages dépend du type de mémoire

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.04.01	BR	Sans fil	Conception du réseau	Description technique	Non	Le fournisseur de service doit être en mesure de garantir que sa documentation relative à l'architecture de la Solution d'Automatisation décrivant les systèmes sans fil est à jour pour les éléments suivants. 1) Échange de données entre un réseau de Niveau 1 et un instrument sans fil, 2) Échange de données entre un réseau de Niveau 2 et un réseau de Niveau 3 par l'intermédiaire d'une liaison sans fil sécurisée, 3) Mécanismes de sécurité empêchant un intrus d'accéder à la Solution d'Automatisation à l'aide d'un système sans fil, 4) Mécanismes de sécurité qui limitent l'accès à la Solution d'Automatisation des travailleurs équipés d'appareils sans fil portatifs, 5) Le cas échéant, les mécanismes de sécurité qui assurent la protection de la gestion à distance des systèmes sans fil. NOTE 1 Le terme "Niveau" se rapporte à la position dans le modèle PRM (Purdue Reference Model) normalisé par l'ISA 95 et l'IEC 62264-1 (voir 5.3).	La capacité spécifiée par cette BR est utilisée pour garantir que les réseaux sans fil sont protégés contre toute intrusion non autorisée à la Solution d'Automatisation Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de maintenir à jour sa documentation relative à l'architecture de communication sans fil, incluant les flux de données, les mécanismes de sécurité et l'utilisation de ponts sans fil. NOTE 2 Les zones et les conduits décrits dans l'IEC 62443-3-2 sont souvent utilisés pour définir les limites de sécurité associées à l'accès sans fil aux appareils/stations de travail filaires dans la Solution d'Automatisation.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.04.02	BR	Sans fil	Conception du réseau	Contrôle d'accès	Non	Le fournisseur de service doit être en mesure de garantir que l'accès aux appareils sans fil est protégé par des mécanismes d'authentification et de contrôle d'accès communément acceptés par les communautés de sécurité et d'automatisation industrielle.	Les capacités spécifiées par cette BR et ses RE sont utilisées pour garantir la protection des appareils sans fil et leurs communications contre tout accès non autorisé. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de fournir ou d'utiliser des mécanismes d'authentification et des listes de contrôle d'accès communément acceptés pour empêcher tout accès non autorisé aux appareils sans fil.
SP.04.02	RE(1)	Sans fil	Conception du réseau	Communications	Non	Le fournisseur de service doit être en mesure de garantir que les communications sans fil sont protégées par des mécanismes de chiffrement communément acceptés par les communautés de sécurité et d'automatisation industrielle.	Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir que les réseaux utilisés dans la Solution d'Automatisation emploient les mécanismes communément acceptés pour protéger l'accès aux données pendant la transmission. Cela inclut les communications sans fil entre les appareils et points d'accès sans fil et entre les points d'accès sans fil et d'autres points d'accès sans fil.
SP.04.03	BR	Sans fil	Conception du réseau	Communications	Non	Le fournisseur de service doit être en mesure de garantir que les protocoles sans fil utilisés dans la Solution d'Automatisation satisfont aux normes communément utilisées dans la communauté de sécurité industrielle, ainsi qu'aux réglementations en vigueur.	Les capacités spécifiées par cette BR et ses RE sont utilisées pour donner l'assurance que les réseaux sans fil utilisent des protocoles qui ont été validés pour être utilisés dans les applications industrielles. Cela signifie que le fournisseur de service (1) utilise dans la Solution d'Automatisation une technologie sans fil normalisée communément acceptée et (2) qu'il dispose d'un processus identifiable permettant de garantir que la technologie sans fil utilisée satisfait aux règlementations locales.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.04.03	RE(1)	Sans fil	Conception du réseau	Identificateurs de réseau sans fil	Non	Le fournisseur de service doit être en mesure de garantir que des identificateurs uniques spécifiques à la Solution d'Automatisation sont utilisés pour les réseaux sans fil, et que tous les identificateurs sans fil sont des acronymes descriptifs qui ne sont manifestement pas associés au site du propriétaire d'actif.	La capacité spécifiée par cette RE est utilisée pour donner l'assurance que les réseaux sans fil sont configurés pour empêcher toute identification facile (les identificateurs de réseau ne sont pas manifestes). Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir que chaque réseau sans fil dispose de son propre identificateur (SSID, par exemple) et que ces identificateurs ne permettent pas à un programme d'écoute externe d'identifier le réseau physique sans fil, son emplacement ou son propriétaire. Si les valeurs de l'identificateur sont définies par le propriétaire d'actif, le rôle du fournisseur de service est, le cas échéant, de donner les lignes directrices pour leur définition et/ou l'examen des identificateurs définis.
SP.04.03	RE(2)	Sans fil	Conception du réseau	Connectivité	Non	Le fournisseur de service doit garantir que les appareils sans fil de la Solution d'Automatisation dotés d'adresses IP utilisent l'adressage statique et que leurs mécanismes dynamiques d'attribution d'adresse (DHCP, par exemple) sont désactivés.	La capacité spécifiée par cette RE est utilisée pour donner l'assurance que les réseaux sans fil sont configurés pour empêcher: 1) l'utilisation d'adresses d'appareil non autorisées, 2) les attaques suite à l'épuisement du protocole DHCP (en désactivant l'utilisation du protocole DHCP). Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir que des mécanismes dynamiques d'attribution d'adresse ne peuvent pas modifier les adresses d'un appareil sans fil doté d'une adresse IP.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.05.01	BR	SIS	Appréciation du risque	Vérification	Non	Le fournisseur de service doit être en mesure de vérifier que les revues d'architecture de sécurité et/ou les appréciations des risques de sécurité des communications du système équipé pour la sécurité (SIS) utilisé dans la Solution d'Automatisation ont été menées et gérées.	La capacité spécifiée par cette BR est utilisée pour donner l'assurance que les risques de sécurité associés au système SIS sont gérés. Cela signifie que le fournisseur de service peut prouver que la sécurité des communications internes et externes du système équipé pour la sécurité, identifiée par des appréciations des risques/des revues de sécurité a été gérée. En règle générale, la revue est réalisée sur un système équipé pour la sécurité intégré/produit de système de commande sous la direction du fournisseur du système de commande selon les dispositions du 8.2.4 de l'IEC 61511-1, et les problèmes détectés sont gérés par le fournisseur. Dans certains cas, l'atténuation des risques est confiée au fournisseur de service dans le cadre de l'installation/maintenance de la Solution d'Automatisation. Dans ces cas, cette exigence implique que le fournisseur de service garantisse que des mesures d'atténuation appropriées pour la Solution d'Automatisation sont déterminées et mises en œuvre.
SP.05.02	BR	SIS	Conception du réseau	Communications	Non	Le fournisseur de service doit être en mesure de garantir que les communications critiques pour la sécurité du système équipé pour la sécurité (SIS) et les autres communications de la Solution d'Automatisation sont physiquement et logiquement séparées, et qu'une défaillance au niveau de leur interface n'a aucune incidence sur l'aptitude du SIS à réaliser ses fonctions de sécurité. NOTE Cette exigence n'implique pas que les communications non critiques pour la sécurité entre le système équipé pour la sécurité et le BPCS (téléchargements de configuration, surveillance de l'état, journalisation, par exemple) soient séparées d'autres communications de la Solution d'Automatisation.	La capacité spécifiée par cette BR est utilisée pour garantir que les communications critiques pour la sécurité du SIS ne sont pas affectées par les communications non critiques pour la sécurité. Cela signifie que le fournisseur de service est en mesure d'isoler logiquement ou physiquement la communication de sécurité fonctionnelle d'un autre trafic de la Solution d'Automatisation pour SIL 1 et au-delà (voir l'IEC 61508). Cela signifie également que le fournisseur de service peut prouver que les contremesures prises pour isoler les communications de sécurité fonctionnelles n'ont pas d'impact sur les performances ou le fonctionnement du système équipé pour la sécurité (SIS). Les appréciations des risques, les zones (segments de réseau) et les conduits (connexions entre des segments de réseau) décrits dans l'IEC 62443-3-2 peuvent être utilisés dans la définition des exigences.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.05.03	BR	SIS	Conception du réseau	Communications	Non	Le fournisseur de service doit être en mesure de garantir que les applications, y compris les applications d'accès distant (par exemple, RDP) au Niveau 3 et au-dessus ne peuvent pas établir (ou sinon disposent) de connexions au système équipé pour la sécurité. NOTE Le terme "Niveau" se rapporte à la position dans le modèle PRM (Purdue Reference Model) normalisé par l'ISA 95 et l'IEC 62264-1 (voir 5.3).	La capacité spécifiée par cette BR est utilisée pour garantir que le système équipé pour la sécurité (SIS) n'est pas en mesure d'être affecté par des appareils/applications du Niveau 3. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir que le système équipé pour la sécurité ne peut pas être connecté, physiquement ou logiquement, au Niveau 3 ou au-dessus. Il n'est pas permis aux applications au-dessus du Niveau 2 de se connecter directement au système équipé pour la sécurité.
SP.05.04	BR	SIS	Conception du réseau	Communications	Non	Le fournisseur de service doit être en mesure de garantir qu'aucune communication critique pour la sécurité n'est établie entre le système équipé pour la sécurité et les applications qui lui sont extérieures (les applications de système de commande, par exemple).	La capacité spécifiée par cette BR est utilisée pour garantir qu'une limite de confiance est établie entre le système équipé pour la sécurité (SIS) et le BPCS qui ne permet pas aux communications critiques pour la sécurité de dépasser la limite de confiance. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir qu'aucune communication critique pour la sécurité (données et /ou commandes, par exemple) n'est transférée entre le système équipé pour la sécurité et les applications qui lui sont extérieures. Cette exigence vise à empêcher que le trafic issu de sources extérieures au système équipé pour la sécurité ne compromette les fonctions de ce dernier.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.05.05	BR	SIS	Appareils – Stations de travail	Communications	Non	Le fournisseur de service doit être en mesure de garantir que toutes les communications entre le Niveau 3 et niveaux supérieurs et les systèmes d'alerte précoce du système équipé pour la sécurité (SIS) qui se situent à l'extérieur du SIS passent par un appareil de sécurité de réseau ou un mécanisme équivalent, qui sépare le Niveau 2 du Niveau 3 ou niveaux supérieurs. NOTE Le terme "Niveau" se rapporte à la position dans le modèle PRM (Purdue Reference Model) normalisé par l'ISA 95 et l'IEC 62264-1 (voir 5.3).	La capacité spécifiée par cette BR permet d'utiliser les appareils de sécurité de réseau pour garantir que seules les communications autorisées entre les applications de Niveau 3 et les stations de travail techniques du système équipé pour la sécurité (SIS) situées à l'extérieur du SIS sont autorisées. L'accès à partir des applications de Niveau 3 aux stations de travail techniques qui se situent à l'intérieur du SIS est interdit par le SP.05.03 BR. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir que toutes les communications entre la station de travail technique du système équipé pour la sécurité et les applications de Niveau 3 (et niveaux supérieurs) passent par un appareil de sécurité de réseau ou un mécanisme équivalent, qui connecte le Niveau 2 et le Niveau 3 (ou niveaux supérieurs).
SP.05.05	RE(1)	SIS	Appareils – Stations de travail	Communications	Non	Le fournisseur de service doit être en mesure de garantir que l'accès distant (RDP, par exemple) au système d'alerte précoce du système équipé pour la sécurité de la Solution d'Automatisation est impossible.	La capacité spécifiée par cette RE est définie pour empêcher que les stations de travail techniques du SIS soient exploitées par l'intermédiaire des connexions d'accès distant. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir qu'aucun accès distant n'est installé (1) ou que tout accès distant est désactivé (2) sur les stations de travail techniques du système équipé pour la sécurité (RDP, par exemple). Une appréciation du risque peut être utilisée pour déterminer le risque lié à l'autorisation d'accès distant au système d'alerte précoce du système équipé pour la sécurité. NOTE Voir l'IEC 62443-3-2 pour des lignes directrices sur les éléments à considérer dans de telles appréciations des risques en matière de cybersécurité.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.05.06	BR	SIS	Appareils – Stations de travail	Connectivité	Non	Le fournisseur de service doit être en mesure de garantir que tout accès au SIS de la Solution d'Automatisation passe: 1) par une passerelle de Niveau 2 dédiée au SIS et lui étant physiquement connectée (par exemple, par une liaison dédiée), et /ou 2) à partir d'un système d'alerte précoce du SIS qui est physiquement connecté au SIS. Si le système d'alerte précoce du SIS n'est pas physiquement connecté au SIS, sa seule option est de communiquer au SIS par la passerelle décrite en (1).	La capacité spécifiée par cette BR est utilisée pour limiter le nombre de chemins d'accès physique au SIS, et donc pour réduire sa surface d'attaque. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir que le SIS n'est physiquement connecté: 1) qu'au système d'alerte précoce du SIS et/ou 2) qu'à une passerelle utilisée uniquement pour assurer l'accès au SIS à partir du Niveau 2. Si le premier cas n'est pas utilisé, le système d'alerte précoce du SIS se connecte à une passerelle qui lance des requêtes au SIS au nom du système d'alerte précoce du SIS.
SP.05.07	BR	SIS	Appareils – Stations de travail	Fonctionnalité minimale	Non	Le fournisseur de service doit être en mesure de garantir que le système d'alerte précoce du système équipé pour la sécurité (SIS) de la Solution d'Automatisation est limité à l'exécution des fonctions du système équipé pour la sécurité.	La capacité spécifiée par cette BR est utilisée pour réduire la possibilité que le système d'alerte précoce du SIS contienne des logiciels susceptibles de nuire, de façon intentionnelle ou accidentelle, au SIS. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir que les stations de travail techniques du système équipé pour la sécurité sont dédiées à ce dernier, et qu'elles ne sont pas utilisées à d'autres fins dans le système de commande.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.05.08	BR	SIS	Appareils – Sans fil	Connectivité	Non	Le fournisseur de service doit être en mesure de vérifier que les appareils sans fil ne sont pas admis dans le cadre des fonctions de sécurité du SIS.	La capacité spécifiée par cette BR est utilisée pour empêcher des attaques sans fil contre le SIS car les appareils sans fil ne sont pas limités par des périmètres de sécurité physique ni par une mise en œuvre physique. Par exemple, une machine de la classe station de travail / serveur située à l'extérieur du périmètre de sécurité physique, configurée avec l'interface d'un appareil sans fil et capable de se connecter au réseau d'appareils sans fil, peut représenter une menace pour le SIS. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de vérifier que les communications des appareils sans fil ne sont pas utilisées dans le système équipé pour la sécurité (SIS).
SP.05.09	BR	SIS	Interface utilisateur	Mode de configuration	Non	Le fournisseur de service doit être en mesure de garantir que la Solution d'Automatisation fournit une interface utilisateur pour l'activation et la désactivation du mode de configuration SIS. Lorsqu'elle est verrouillée, cette interface doit empêcher le SIS d'être configuré. NOTE En règle générale, cette interface empêche la transmission des messages de configuration au SIS.	Les capacités spécifiées par cette BR et ses RE sont utilisées pour empêcher tout accès de configuration au SIS au cours du fonctionnement normal par un mécanisme qui exige de déverrouiller le SIS pour le configurer et de le verrouiller dans tous les autres cas. Cela signifie que le fournisseur de service est en mesure de garantir que le système équipé pour la sécurité peut être verrouillé afin d'éviter de modifier la configuration, et déverrouillé pour pouvoir apporter ces modifications. Les verrous peuvent être des touches contacts physiques ou des verrous contrôlés par logiciel. Toutefois, lorsqu'ils sont mis en œuvre, ils permettent de pouvoir verrouiller le système équipé pour la sécurité afin d'éviter les modifications accidentelles ou malveillantes.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.05.09	RE(1)	SIS	Interface utilisateur	Mode de configuration	Non	Le fournisseur de service doit être en mesure de garantir que la Solution d'Automatisation assure la mise en œuvre matérielle de l'interface exigée par le SP.05.09 BR, laquelle peut être physiquement verrouillée lorsque le mode de configuration est désactivé.	La capacité spécifiée par cette RE est définie pour garantir qu'une intervention humaine volontaire soit en mesure d'activer la configuration du SIS (le maintien d'une touche physique à l'état ouvert (déverrouillé) par exemple) pendant la modification de la configuration, afin de renforcer l'assurance que des modifications accidentelles de la configuration du SIS ne peuvent se produire. Cela signifie que le fournisseur de service est en mesure de garantir que le système équipé pour la sécurité dispose d'une interface matérielle qui peut être désactivée pour empêcher les modifications de configuration. Lorsque l'interface matérielle (une touche contact physique, par exemple) est verrouillée physiquement (en retirant la clé, par exemple), le mode de configuration est désactivé.
SP.05.09	RE(2)	SIS	Interface utilisateur	Mode de configuration	Non	Le fournisseur de service doit être en mesure de demander à un tiers indépendant de vérifier qu'il n'est pas possible de modifier la configuration du système équipé pour la sécurité lorsque l'interface matérielle décrite dans SP.05.09 RE(1) est verrouillée en mode de configuration "disable" (désactiver).	La capacité spécifiée par cette RE est définie pour ajouter un niveau supplémentaire d'assurance que le mécanisme de verrouillage physique fonctionne comme prévu. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de fournir un rapport rédigé par un tiers qui a vérifié que le mécanisme de verrouillage de configuration du système équipé pour la sécurité fonctionne. Ce rapport peut être initié (en vertu d'un contrat, par exemple) par le fournisseur du système de commande pour la Solution d'Automatisation ou par le fournisseur de service. Cette vérification peut se dérouler avant la livraison du produit à la Solution d'Automatisation (dans le cadre de la vérification des produits) ou après la livraison de l'interface matérielle (dans le cadre des activités de la Solution d'Automatisation du fournisseur de service.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.06.01	BR	Gestion de la configuration	Conception du réseau	Connectivité	Non	Le fournisseur de service doit être en mesure de fournir des schémas / documents d'infrastructure logique et physique exacts de la Solution d'Automatisation, y compris de ses appareils de réseau, interfaces internes et interfaces externes. Il faut que la documentation et les dessins soient considérés comme une représentation exacte de la Solution d'Automatisation.	Les capacités spécifiées par cette BR et ses RE sont utilisées pour garantir qu'une représentation exacte de l'architecture réseau de la Solution d'Automatisation est documentée et disponible pour les activités relatives à la sécurité, telles que les appréciations des risques et l'analyse des activités d'investigation numérique. Cela signifie que le fournisseur dispose d'un processus identifiable permettant de maintenir sa documentation d'architecture réseau à jour. L'architecture réseau inclut chaque segment de réseau, les appareils de réseau utilisés pour interconnecter les segments de réseau et une identification de toutes les interfaces réseau internes à la Solution d'Automatisation et celles qui connectent la Solution d'Automatisation à des réseaux externes. Les interfaces réseau peuvent être identifiées au moyen de diverses techniques, y compris des adresses Ethernet (c'est-à-dire des adresses MAC), des adresses IP et des identificateurs de carte d'interface réseau. Il s'agit de fournir suffisamment d'informations les concernant afin de les identifier sans ambigüité. Les appréciations des risques, les zones (segments de réseau) et les conduits (connexions entre des segments de réseau) décrits dans l'IEC 62443-3-2 peuvent être utilisés dans le développement de l'architecture réseau.
SP.06.01	RE(1)	Gestion de la configuration	Conception du réseau	Connectivité	Non	Le fournisseur de service doit être en mesure de maintenir à jour les documents de connexion et de configuration de l'équipement conforme à l'exécution et installé.	Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de maintenir sa documentation à jour, afin de décrire les appareils connectés à chaque segment de réseau dans la Solution d'Automatisation. EXEMPLE Pour un appareil Ethernet, la documentation inclurait l'adresse de réseau et le commutateur auquel l'appareil est connecté, ainsi qu'une copie du fichier de téléchargement utilisé pour configurer l'appareil.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.06.02	BR	Gestion de la configuration	Appareils – Tous	Registre d'inventaire	Non	Le fournisseur de service doit être en mesure de créer et de gérer un registre d'inventaire, y compris les numéros de version et numéros de série, de tous les appareils et leurs composants logiciels dans la Solution d'Automatisation dont est responsable le fournisseur de service.	La capacité spécifiée par cette BR est utilisée pour garantir qu'un inventaire de composants est tenu à jour pour pouvoir déterminer si un composant dans la Solution d'Automatisation est autorisé, et également pour être en mesure de déterminer si une vulnérabilité nouvellement détectée dans le secteur est applicable à la Solution d'Automatisation. Par exemple, si une vulnérabilité à un niveau de version/correctif spécifique est détectée, il convient de pouvoir consulter le registre d'inventaire de la Solution d'Automatisation pour déterminer si la vulnérabilité est applicable à des appareils/composants utilisés dans la Solution d'Automatisation. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de fournir la documentation pour tous les composants de la Solution d'Automatisation dont il est responsable. Les caractéristiques incluent des informations telles que les numéros de modèle, de version et de série. La documentation peut inclure des rapports, des données de configuration générées automatiquement, des captures d'écran, etc.
SP.06.03	BR	Gestion de la configuration	Appareils-Contrôle et instruments	Vérification	Non	Le fournisseur de service doit être en mesure de vérifier que les appareils filaires et sans fil utilisés pour le contrôle et les instruments ont été correctement configurés avec leurs valeurs approuvées	La capacité spécifiée par cette BR est utilisée pour vérifier l'intégrité des configurations de l'appareil. Il s'agit de pouvoir détecter les modifications de configuration non autorisées ou erronées. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de vérifier que les paramètres de configuration de l'appareil ont été correctement téléchargés/écrits dans l'appareil. EXEMPLE Les valeurs de paramètre de configuration peuvent être confirmées en les visualisant à partir d'une station de travail.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.07.01	BR	Accès distant	Outils et logiciels de sécurité	Connectivité	Non	Le fournisseur de service doit être en mesure de garantir que les applications d'accès distant utilisées dans la Solution d'Automatisation sont communément acceptées par les communautés de sécurité et d'automatisation industrielle.	La capacité spécifiée par cette BR est utilisée pour garantir que les applications d'accès distant fournissent des niveaux acceptables de protection à la Solution d'Automatisation. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir que toutes les applications d'accès distant sont prises en charge par des mécanismes d'accès distant communément acceptés (RDP, par exemple). Les clients d'accès distant peuvent être fournis par le client et/ou le fournisseur de service.
SP.07.02	BR	Accès distant	Outils et logiciels de sécurité	Description technique	Non	Le fournisseur de service doit être en mesure de fournir les instructions détaillées pour l'installation, la configuration, le fonctionnement et la fin des applications d'accès distant utilisées dans la Solution d'Automatisation.	La capacité spécifiée par cette BR est utilisée pour garantir que les applications d'accès distant fournissent des niveaux acceptables de protection à la Solution d'Automatisation. Cela signifie que le fournisseur de service dispose de la documentation pour l'installation, la configuration et le fonctionnement des applications d'accès distant dont il recommande l'utilisation dans la Solution d'Automatisation. Le fournisseur de service est également tenu de donner des instructions au propriétaire d'actif pour mettre fin à ces connexions. Le fournisseur de service n'est pas autorisé à établir des connexions d'accès distant auxquelles le propriétaire d'actif ne peut pas mettre fin.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.07.03	BR	Accès distant	Outils et logiciels de sécurité	Description technique	Non	Le fournisseur de service doit être en mesure de donner des informations relatives à toutes les connexions d'accès distant proposées au propriétaire d'actif, incluant, pour chaque connexion: 1) leur objet, 2) l'application d'accès distant qui est à utiliser, 3) la manière dont la connexion sera établie (par Internet ou VPN, par exemple), et 4) l'emplacement et l'identification du client distant.	La capacité spécifiée par cette BR est utilisée pour garantir que l'accès distant à la Solution d'Automatisation est documenté et géré de manière à contrecarrer les tentatives non autorisées d'accéder à distance à la Solution d'Automatisation. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de définir les détails de toutes les connexions d'accès distant proposées, et d'en informer le propriétaire d'actif. Il est nécessaire de documenter l'emplacement proposé du client d'accès distant pour permettre au propriétaire d'actif d'examiner et approuver/ rejeter l'accès distant à partir d'emplacements spécifiques. Dans certains cas, l'emplacement proposé peut indiquer une ''itinérance'' permettant d'utiliser des appareils portables comme clients. Il n'est pas prévu que la Solution d'Automatisation puisse vérifier automatiquement l'emplacement physique du client en cours d'exécution.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.07.04	BR	Accès distant	Outils et logiciels de sécurité	Approbation	Non	Le fournisseur de service doit être en mesure de garantir qu'il obtient l'approbation du propriétaire d'actif avant l'utilisation de chacune et de l'ensemble des connexions d'accès distant.	La capacité spécifiée par cette BR est utilisée pour garantir que toutes les connexions d'accès distant à la Solution d'Automatisation sont autorisées par le propriétaire d'actif. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de n'utiliser que les connexions qui ont été approuvées par le propriétaire d'actif. Il peut s'agir de connexions d'accès distant utilisateur/système ou système/système, qui peuvent passer par Internet et/ou inclure l'utilisation de modems, et/ou qui peuvent être fournies et gérées par le propriétaire d'actif. Les exigences de gestion de ces connexions et le temps dont a besoin le propriétaire d'actif pour approuver les connexions sont hors du domaine d'application de cette exigence. De plus, le propriétaire d'actif peut demander au fournisseur de service d'assurer ou de maintenir les connexions, et peut fournir les exigences appropriées à cet instant. Par exemple, le propriétaire d'actif peut ne pas autoriser l'utilisation du protocole TCP/IP sur des connexions externes qui utilisent des modems. Une appréciation du risque, telle que décrite dans l'IEC 62443-3-2, peut être utilisée pour définir ces exigences, y compris s'il convient de chiffrer ou non la connexion, et si un modem peut être utilisé ou non pour assurer la connexion et, par conséquent, s'il convient de déconnecter le modem lorsqu'il n'est pas utilisé, et s'il convient de pouvoir utiliser le modem comme un routeur.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.07.04	RE(1)	Accès distant	Protection des données	Cryptographie	Non	Le fournisseur de service doit être en mesure de garantir que toutes les connexions d'accès distant établies sur Internet ou sur d'autres supports accessibles au public que le fournisseur de service utilise pour prendre en charge l'accès distant à la Solution d'Automatisation (à partir d'une installation du fournisseur de service, par exemple) sont authentifiées et chiffrées.	La capacité spécifiée par cette RE est définie pour garantir que toutes les connexions utilisées pour prendre en charge l'accès distant à la Solution d'Automatisation par le fournisseur de service sont protégées. Les fournisseurs de service offrent souvent des services de prise en charge à distance et de dépannage /diagnostic à la Solution d'Automatisation. Cela signifie que le fournisseur de service dispose d'un processus identifiable lui permettant d'utiliser des liaisons chiffrées (des VPN, par exemple) pour l'accès distant à la Solution d'Automatisation sur Internet (par exemple, à partir de ses installations ou d'autres emplacements distants). L'authentification est exigée pour garantir que seuls les clients distants autorisés peuvent accéder à la Solution d'Automatisation. En général, cette exigence relative à l'accès distant à la Solution d'Automatisation impose au fournisseur de service de prendre en charge des activités telles que la prise en charge à distance.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.08.01	BR	Gestion des événements	Événements – Failles de sécurité	Génération de réponses	Non	Le fournisseur de service doit être en mesure de gérer les incidents de cybersécurité qui affectent la Solution d'Automatisation, à savoir: 1) la détection des failles et incidents de cybersécurité, 2) le signalement des incidents de cybersécurité au propriétaire d'actif, 3) la réponse aux failles et incidents de cybersécurité, y compris la prise en charge d'une équipe de réponse aux incidents. NOTE 1 La journalisation des événements liés à la sécurité est abordée par le SP.08.02 BR. NOTE 2 La journalisation et le signalement des alarmes et des événements sont abordés par le SP.08.03 BR.	Les capacités spécifiées par cette BR et ses RE sont utilisées pour garantir que les incidents de sécurité relatifs à la Solution d'Automatisation sont gérés depuis leur détection jusqu'à leur élimination afin de maintenir la position des risques de sécurité de la Solution d'Automatisation. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de détecter, de traiter et de signaler des incidents de cybersécurité liés aux composants de la Solution d'Automatisation dont il est responsable. Les procédures de traitement des incidents du fournisseur définissent ce qui constitue un incident, quels incidents sont significatifs et dans quelles conditions ils sont signalés au propriétaire d'actif. La mise en œuvre du traitement des incidents peut être contrôlée dans le cadre d'accords particuliers entre le propriétaire d'actif et le fournisseur de service, tels que les accords de confidentialité et/ou d'autres documents contractuels entre le propriétaire d'actif et le fournisseur de service. Ces documents contractuels identifient souvent les données propriétaires à protéger et les types de failles à signaler. En règle générale, le processus d'identification des incidents inclut (1) l'analyse et la corrélation des événements, et (2) l'examen et le tri des failles obtenues et des éventuels incidents donnant lieu à des incidents. SP.03.03 BR aborde le traitement des vulnérabilités qui ont pu être décelées par ce processus ou par d'autres processus. Dans la plupart des cas, la reconnaissance de la survenue d'une faille et de la perte qui peut en résulter peut être difficile et impliquer une part de subjectivité et de jugement. La spécification de ce processus et la définition précise de ce qui constitue un incident n'entrent pas dans le domaine d'application de ces exigences.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
							Pour les exigences relatives au traitement et au signalement des incidents liés au développement des produits, qui peuvent compléter les capacités du fournisseur de service en matière de traitement des incidents, voir l'IEC 62443-4-1 et l'ISO/IEC 30111.
SP.08.01	RE(1)	Gestion des événements	Événements – Failles de sécurité	Génération de rapports	Non	Le fournisseur de service doit être en mesure de garantir que les failles de sécurité qui ont été automatiquement détectées peuvent être signalées par l'intermédiaire d'une interface de communication à laquelle le propriétaire d'actif peut accéder et qui est communément acceptée par les communautés de sécurité et d'automatisation industrielle.	Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de signaler les failles de sécurité qu'il détecte automatiquement. Les failles de sécurité sont à signaler, qu'elles donnent lieu ou non à une perte ou qu'elles soient classées ou non comme un incident. Les failles de sécurité peuvent être automatiquement détectées au moment de leur survenance ou par des activités d'analyse et de corrélations subséquentes des événements (par l'utilisation du module SIEM (Security Information and Event Management), par exemple).
SP.08.02	BR	Gestion des événements	Événements – Liés à la sécurité	Journalisation	Non	Le fournisseur de service doit être en mesure de garantir que la Solution d'Automatisation est configurée de manière à pouvoir écrire tous les événements liés à la sécurité, y compris les activités de l'utilisateur et les activités de gestion de compte, dans un journal d'audit conservé pendant le nombre de jours spécifié par le propriétaire d'actif. NOTE La journalisation et le signalement des événements liés au processus, tels que les modifications des points de consigne et d'autres modifications de données de fonctionnement/configuration sont abordés par le SP.08.03 BR.	Les capacités spécifiées par cette BR et ses RE sont utilisées pour garantir que les journaux d'audit liés à la sécurité sont pris en charge. Les journaux d'audit peuvent être utilisés dans les activités d'investigation numérique (déterminer par qui et à quel moment a été modifié un compte utilisateur, par exemple) et de corrélation des événements qui peuvent donner lieu à une identification d'incident de sécurité. Les journaux d'audit exigent un niveau plus élevé de protection de l'intégrité que celui des journaux d'événements classiques. Ils assurent la protection contre les déclarations de répudiation de responsabilité pour une action donnée. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de fournir un journal d'audit pour les événements liés à la sécurité qui incluent les connexions et déconnexions réussies et non valides, la création, la modification ou la suppression de comptes utilisateurs, entre autres.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.08.02	RE(1)	Gestion des événements	Événements – Liés à la sécurité	Génération de rapports	Non	Le fournisseur de service doit être en mesure de garantir que les données et événements liés à la sécurité peuvent être consulté(e)s par l'intermédiaire d'une ou de plusieurs interfaces communément acceptées par les communautés de sécurité et d'automatisation industrielle.	Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir que le propriétaire d'actif peut collecter les données et événements de sécurité sur le réseau. Les interfaces communément acceptées incluent les interfaces qui prennent en charge l'invitation à émettre (lectures SNMP, par exemple), la génération de rapport asynchrone (trappes SNMP, par exemple) et la journalisation (Syslog, Syslog-ng et CEF (Common Event Format), par exemple). L'utilisation des interfaces communément acceptées facilite l'intégration des progiciels prêts à l'emploi qui collectent et analysent les données et événements. EXEMPLE En règle générale, les appareils de réseau gèrent une base de données MIB SNMP contenant les données liées à la sécurité accessibles à l'aide du protocole SNMP.
SP.08.02	RE(2)	Gestion des événements	Événements – Liés à la sécurité	Journalisation	Non	Le fournisseur de service doit être en mesure de vérifier, en simulant un événement lié à la sécurité approuvé par le propriétaire d'actif, que les événements liés à la sécurité peuvent être écrits dans un journal d'audit.	Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de vérifier que les mécanismes utilisés pour journaliser et signaler les événements liés à la sécurité fonctionnent comme indiqué dans le SP 08.02 BR et SP 08.02 RE(1). Les journaux d'audit exigent un niveau plus élevé de protection de l'intégrité que celui des journaux d'événements classiques. Ils assurent la protection contre les déclarations de répudiation de responsabilité pour une action donnée.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.08.03	BR	Gestion des événements	Événements – Alarmes et événements	Journalisation	Non	Le fournisseur de service doit être en mesure de garantir que la Solution d'Automatisation est configurée pour journaliser les événements liés au processus et les signaler à l'opérateur, comme exigé par le propriétaire d'actif. Les types d'événements incluent les changements d'état/les changements de condition de fonctionnement/les changements de configuration qui peuvent être dus à des opérations manuelles ou automatisées (celles sans intervention humaine). NOTE 1 La journalisation des événements liés à la sécurité est abordée par le SP.08.02 BR.	Les capacités spécifiées par cette BR et ses RE sont utilisées pour garantir que les journaux d'événement liés au processus sont pris en charge. Les journaux d'événements peuvent être utilisés dans les activités d'investigation numérique (déterminer par qui et à quel moment a été modifié un point de consigne, par exemple) et de corrélation des événements qui peuvent donner lieu à une identification d'incident de sécurité. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir que la Solution d'Automatisation prend en charge la journalisation et la notification des événements liés au processus, et permettant de la configurer pour journaliser les événements indiqués par le propriétaire d'actif et en informer l'opérateur. Les notifications incluent à la fois les notifications d'événements simples et les notifications d'alarmes/alertes. Les alarmes et événements à journaliser et signaler incluent les événements du système d'exploitation et les alarmes et événements du système de commande. Les événements signalés par l'intermédiaire de cette interface peuvent être déterminés pour exiger la protection par une appréciation du risque (voir SP.03.01 BR et ses RE). Voir également SP.03.10 BR et ses RE pour les exigences relatives à la protection des données sensibles. NOTE 2 Les alarmes et alertes, telles que définies par ISA 18.2 ou NAMUR NA102, sont des notifications qui exigent de l'opérateur une réponse (alarme) ou sensibilisation (alerte).
SP.08.03	RE(1)	Gestion des événements	Événements – Alarmes et événements	Génération de rapports	Non	Le fournisseur de service doit être en mesure de garantir que les alarmes/alertes/événements peuvent être signalés en toute sécurité par l'intermédiaire d'une interface communément acceptée par les communautés de sécurité et d'automatisation industrielle.	Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir que la Solution d'Automatisation est en mesure de signaler les alarmes et événements à des applications externes (un journal centralisé, par exemple) par l'intermédiaire d'une interface communément acceptée qui protège les événements transmis contre les altérations et la divulgation. Cette interface peut prendre en charge les notifications d'événements ou l'invitation à émettre des événements.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.08.04	BR	Gestion des événements	Événements – Alarmes et événements	Robustesse	Non	Le fournisseur de service doit être en mesure de garantir que la Solution d'Automatisation peut résister à l'occurrence quasi simultanée d'un grand nombre d'événements, en général appelés salves d'événements.	La capacité spécifiée par cette BR est utilisée pour garantir que la Solution d'Automatisation ne fait pas l'objet d'un refus de service pendant des salves d'événements. Les caractéristiques des salves d'événements (le nombre d'événements/seconde, par exemple) dépendent en général du nombre d'appareils de commande et d'instrumentation dans la Solution d'Automatisation et de la nature du processus physique. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir qu'il est en mesure de configurer la Solution d'Automatisation avec des composants qui la protègent contre les salves d'événements. L'essai de robustesse est souvent effectué pour prouver cette assurance.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.09.01	BR	Gestion des comptes	Comptes – Comptes utilisateurs et comptes de service	Administration	Non	Le fournisseur de service doit être en mesure de garantir que la Solution d'Automatisation prend en charge: 1) l'utilisation d'une seule base de données intégrée, qui peut être répartie ou redondante, pour la définition et la gestion des comptes utilisateurs et des comptes de service, 2) la restriction de la gestion des comptes aux utilisateurs autorisés 3) l'accès décentralisé à cette base de données pour la gestion des comptes, 4) la mise en œuvre décentralisée des paramètres du compte (mots de passe, droits d'accès au système d'exploitation et listes de contrôle d'accès, par exemple) définis dans cette base de données.	La capacité spécifiée par cette BR est utilisée pour simplifier la gestion des comptes utilisateurs pour la Solution d'Automatisation constituée de plusieurs stations de travail et de plusieurs serveurs. Sans ces capacités, la gestion séparée des comptes par des stations de travail et des serveurs individuels résulte souvent en des incohérences qui donnent lieu à un refus de service aux ressources et/ou l'accès inapproprié aux ressources. Cela signifie que le fournisseur de service est en mesure de garantir que la Solution d'Automatisation fournit un système de gestion des comptes qui: 1) comporte une seule base de données qui peut être répartie ou redondante, conformément aux exigences de la Solution d'Automatisation, 2) permet à des utilisateurs autorisés uniquement de définir et gérer des comptes, y compris des comptes utilisateurs, administrateurs/superutilisateurs et des comptes de service (c'est-à-dire des comptes qui ne prévoient pas une connexion interactive), 3) permet à des administrateurs de gérer des comptes à partir d'un ensemble spécifié de stations de travail/serveurs dans la Solution d'Automatisation, et pas simplement à partir d'une station de travail unique dédiée, 4) répartit la mise en œuvre des listes de contrôle et droits d'accès aux comptes à l'emplacement où l'accès ou le droit est à exécuter. Des exemples de ce type de gestion de compte incluent les technologies LDAP (Lightweight Directory Access Protocol) telles que WIndows Active Directory. Voir l'IEC 62443-3-3 pour les exigences liées à la sécurité des systèmes utilisés dans la Solution d'Automatisation.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.09.02	BR	Gestion des comptes	Comptes – Comptes utilisateurs et comptes de service	Administration	Non	Le fournisseur de service doit être en mesure de garantir que les comptes uniques peuvent être créés et gérés pour les utilisateurs.	La capacité spécifiée par cette BR est utilisée pour empêcher les utilisateurs d'avoir à partager l'utilisation des comptes, c'est-à-dire en possédant un compte séparé. Cela signifie que le fournisseur de service dispose d'un processus identifiable de création et de gestion d'un compte utilisateur unique pour chaque utilisateur de la Solution d'Automatisation.
SP.09.02	RE(1)	Gestion des comptes	Comptes – Comptes utilisateurs et comptes de service	Description technique	Oui	Le fournisseur de service doit fournir la documentation au propriétaire d'actif permettant: 1) d'identifier tous les comptes utilisateurs et comptes de service par défaut 2) de décrire les outils et procédures utilisé(e)s pour initialiser/réinitialiser les mots de passe de tous les comptes utilisateurs et comptes de service par défaut.	La capacité spécifiée par cette RE est définie pour garantir qu'il n'y a aucun compte caché ni aucun mot de passe qui ne peut être modifié. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de générer une liste de tous les comptes utilisateurs et comptes de service, et de fournir les instructions au propriétaire d'actif pour décrire la manière de changer leurs mots de passe. Pour les comptes utilisés par des services et des serveurs (serveur DCOM, par exemple), la modification d'un mot de passe peut impliquer une ou plusieurs des opérations suivantes: 1) modification du mot de passe pour le compte, 2) modification du mot de passe "de connexion" dans le ou les services qui s'exécutent dans le cadre du compte, 3) modification du mot de passe utilisé par d'autres processus logiciels qui se connectent à d'autres processus utilisant le compte.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.09.02	RE(2)	Gestion des comptes	Comptes – Comptes utilisateurs et comptes de service	Administration	Non	Le fournisseur de service doit être en mesure de garantir que, si un compte/mot de passe est automatiquement généré pour un utilisateur (autres que des opérateurs ou des groupes de services), le compte et le mot de passe générés sont uniques.	La capacité spécifiée par cette RE est définie pour garantir que le même mot de passe n'est pas généré pour plusieurs comptes utilisateurs, autres que ceux relatifs à l'opérateur et à des groupes de services. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de vérifier que la Solution d'Automatisation ne génère pas le même mot de passe pour deux utilisateurs différents, et que chaque compte utilisateur généré est unique et comporte un identifiant unique. Cette exigence ne s'applique pas aux Solutions d'Automatisation qui ne génèrent pas de comptes et de mots de passe pour des utilisateurs individuels.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.09.02	RE(3)	Gestion des comptes	Comptes – Comptes utilisateurs et comptes de service	Expiration	Non	Le fournisseur de service doit être en mesure de garantir que les comptes de service, les comptes de connexion automatique et les comptes d'opérateur, et les autres comptes exigés pour des fonctions essentielles et/ou des opérations continues, ou tel qu'il est exigé par le propriétaire d'actif ont été configurés pour ne jamais expirer ni se désactiver automatiquement.	La capacité spécifiée par cette RE est définie pour empêcher les services, les opérateurs, les stations de travail configurés pour la connexion automatique et d'autres comptes exigés, d'être soumis à un refus de service parce que leurs comptes ont expiré ou sont automatiquement désactivés. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir que les comptes permanents dans la Solution d'Automatisation (les comptes de service, les comptes de connexion automatique et les comptes d'opérateur) sont configurés de manière à ne pas expirer ni être automatiquement désactivés ou supprimés. En règle générale, les comptes d'opérateur sont des comptes utilisateurs individuels configurés avec des droits d'accès opérateur qui assurent la visibilité dans l'environnement physique (le processus, par exemple) sous contrôle. Cette exigence n'empêche pas de supprimer ou de désactiver les comptes permanents en fonction d'actions explicites prises par un administrateur. Une mesure communément recommandée pour les systèmes basés sur Unix est de configurer le compte principal pour utiliser l'enveloppe fausse ou ''sans connexion'' (rejetant effectivement ainsi toutes les connexions à l'aide de ce compte) et créant un surnom différent pour le compte principal destiné à être utilisé par le personnel administratif autorisé. NOTE Voir SP.03.01 BR et ses RE pour l'évaluation et la gestion des risques associés aux comptes qui n'expirent pas.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.09.02	RE(4)	Gestion des comptes	Comptes - Administrateur	Fonctionnalité minimale	Non	Le fournisseur de service doit être en mesure de garantir que le compte administrateur intégré est désactivé, et si cela s'avère impossible, que le compte administrateur est renommé ou difficile à exploiter.	La capacité spécifiée par cette RE est définie pour empêcher les pirates d'obtenir des droits d'accès administratifs en utilisant le compte administrateur intégré. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de désactiver ou de renommer le compte administrateur intégré ou, si aucune de ces opérations n'est possible, d'en rendre difficile sa reconnaissance et son exploitation. L'accès à un compte administrateur intégré permet aux logiciels malveillants de potentiellement utiliser ce compte et de prendre le contrôle du système. NOTE Le changement de nom n'est pas assez efficace car le système d'exploitation ne peut pas modifier l'identificateur sous-jacent pour le compte.
SP.09.03	BR	Gestion des comptes	Comptes – Valeur par défaut	Fonctionnalité minimale	Non	Le fournisseur de service doit être en mesure de garantir que les comptes par défaut du système inutilisés ont été supprimés ou désactivés.	La capacité spécifiée par cette BR est utilisée pour empêcher les pirates d'avoir accès à la Solution d'Automatisation par l'intermédiaire des comptes par défaut du système. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de supprimer les comptes (intégrés) par défaut du système qui ne sont pas nécessaires pour la Solution d'Automatisation. Les comptes intégrés sont en général installés lorsque de nouveaux ordinateurs (des stations de travail, par exemple) sont ajoutés à la Solution d'Automatisation ou que leur logiciel est installé ou réinstallé. Cette exigence s'applique à tous les comptes par défaut du système, qu'ils soient installés avec le système d'exploitation, avec le système de commande ou avec le logiciel associé. Le fournisseur de service nécessite de disposer d'un processus permettant de garantir que les comptes intégrés inutiles sont retirés.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.09.04	BR	Gestion des comptes	Comptes – Utilisateur	Fonctionnalité minimale	Non	Le fournisseur de service doit être en mesure de garantir que tous les comptes utilisateurs sont supprimés s'ils ne sont plus nécessaires, à savoir: 1) les comptes temporaires sous le contrôle du fournisseur de service, tels que ceux utilisés pour l'intégration et la maintenance, 2) les comptes utilisateurs pour le personnel du fournisseur de service qui n'est plus affecté à la Solution d'Automatisation (voir SP.01.07 BR pour la notification au propriétaire d'actif du retrait du personnel du fournisseur de service de la Solution d'Automatisation).	Les capacités spécifiées par cette BR et ses RE sont utilisées pour empêcher les pirates d'avoir accès à la Solution d'Automatisation par l'intermédiaire des comptes qui ne sont pas nécessaires (comptes des utilisateurs qui ne sont plus affectés à la Solution d'Automatisation, par exemple). Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de supprimer ou de désactiver des comptes créés pour prendre en charge son personnel à l'issue de ses activités ou à la fin de son affectation à la Solution d'Automatisation. Il s'agit de garantir que la Solution d'Automatisation ne contient pas ou ne conserve pas les comptes du fournisseur de service, sauf s'ils sont nécessaires.
SP.09.04	RE(1)	Gestion des comptes	Comptes – Utilisateur	Journalisation	Non	Le fournisseur de service doit être en mesure de générer un journal d'audit à l'issue des activités d'intégration/de maintenance, montrant que les comptes utilisés pour la prise en charge de ces activités ont été retirés de la Solution d'Automatisation s'ils ne sont plus nécessaires.	Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de générer un rapport confirmant que les comptes créés pour prendre en charge ses activités ont été supprimés à l'issue de ces activités. Il s'agit de garantir que la Solution d'Automatisation ne contient pas ou ne conserve pas les comptes du fournisseur de service, sauf s'ils sont nécessaires. Voir SP.08.02 BR pour l'exigence de journalisation des événements liés à la sécurité, qui inclut la suppression de ces comptes.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.09.05	BR	Gestion des comptes	Mots de passe	Composition	Non	Le fournisseur de service doit être en mesure de garantir que les politiques relatives aux mots de passe peuvent être définies de sorte que les mots de passe aient une complexité minimale communément acceptée par les communautés de sécurité et d'automatisation industrielle NOTE Au moment de la rédaction de cette exigence, la complexité minimale du mot de passe est: 1) d'au moins huit caractères et 2) d'une combinaison d'au moins trois des quatre jeux de caractères suivants: minuscule, majuscule, valeur numérique et caractères spéciaux (% et #, par exemple).	La capacité spécifiée par cette BR est utilisée pour garantir que le fournisseur de service peut prendre en charge un large éventail de politiques de complexité de mot de passe du propriétaire d'actif. L'utilisation de mots de passe complexes rend plus difficile leur détection. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir que la Solution d'Automatisation prend en charge les mots de passe complexes. La complexité des mots de passe utilisés dans une Solution d'Automatisation spécifique ne relève pas du domaine d'application de cette exigence. Voir l'IEC 62443-3-3 pour les exigences liées à la sécurité des systèmes utilisés dans les Solutions d'Automatisation, et l'IEC 62443-3-2 pour l'utilisation de l'appréciation du risque en vue de faciliter la détermination du niveau de complexité des mots de passe à utiliser dans le cadre d'une Solution d'Automatisation spécifique. Voir également l'IEC 62443-2-1 pour les exigences relatives à la politique des mots de passe pour les propriétaires d'actif.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.09.06	BR	Gestion des comptes	Mots de passe	Expiration	Non	Le fournisseur de service doit être en mesure de garantir que les mots de passe des comptes utilisateurs locaux et au niveau du système (le domaine, par exemple) sont configurés pour expirer automatiquement après avoir été utilisés pendant une période de temps spécifiée par le propriétaire d'actif.	Les capacités spécifiées par cette BR et ses RE sont utilisées pour garantir que les mots de passe peuvent être modifiés régulièrement. Les mots de passe non modifiés augmentent le risque d'être divulgués/détectés et utilisés pour avoir un accès non autorisé au système. De plus, la modification régulière des mots de passe limite la période de temps nécessaire à un pirate pour détecter un mot de passe. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir que les mots de passe peuvent être configurés pour expirer automatiquement après avoir été utilisés pendant le nombre de jours spécifié par le propriétaire d'actif. Le moment et la fréquence de vérification de la période d'expiration du mot de passe par le fournisseur de service sont spécifiques à la Solution d'Automatisation, mais la vérification se déroule en général dans le cadre du processus de transfert et après ou pendant chaque cycle de maintenance. Il convient que la politique de sécurité du propriétaire d'actif définisse la période d'expiration en fonction de l'appréciation du risque, et que cette valeur soit régulièrement revue. Voir l'IEC 62443-3-2 pour plus d'informations sur l'appréciation du risque, l'IEC 62443-3-3 pour les exigences connexes relatives aux capacités de produit des systèmes de commande et l'IEC 62443-2-1 pour les exigences connexes relatives aux propriétaires d'actif. NOTE L'IEC 62443-2-1 ne mentionne pas explicitement d'exigences de durée de vie des mots de passe, mais traite des politiques plus générales en matière de mot de passe.
SP.09.06	RE(1)	Gestion des comptes	Mots de passe	Expiration	Non	Le fournisseur de service doit être en mesure de garantir que les politiques relatives aux mots de passe sont définies pour inviter les utilisateurs à modifier les mots de passe *N* jours avant leur expiration, *N* étant spécifié par le propriétaire d'actif. Cette exigence ne s'applique pas aux mots de passe qui ne sont pas définis pour expirer.	Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir que les utilisateurs sont informés de l'expiration de leurs mots de passe et qu'ils ont donc le temps de les modifier.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.09.07	BR	Gestion des comptes	Mots de passe	Modification	Non	Le fournisseur de service doit être en mesure de garantir que les mots de passe par défaut sont modifiés comme exigé par le propriétaire d'actif.	La capacité spécifiée par cette BR est définie pour empêcher les mots de passe par défaut, qui sont bien connus, d'être utilisés dans la Solution d'Automatisation. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir que les mots de passe par défaut sont modifiés conformément aux exigences du propriétaire d'actif. En règle générale, cette modification a lieu à l'installation, la réinstallation et la réinitialisation/reprise.
SP.09.08	BR	Gestion des comptes	Mots de passe	Réutilisation	Non	Le fournisseur de service doit être en mesure de garantir que les politiques relatives aux mots de passe sont définies pour empêcher les utilisateurs de réutiliser leurs *N* derniers mots de passe, *N* étant spécifié par le propriétaire d'actif.	Les capacités spécifiées par cette BR et ses RE sont définies pour empêcher les utilisateurs de modifier leurs mots de passe pour ensuite les remodifier immédiatement, ce qui signifierait effectivement que leurs mots de passe n'ont pas été modifiés. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de vérifier que la politique de réutilisation de mot de passe est définie sur le nombre spécifié par le propriétaire d'actif.
SP.09.08	RE(1)	Gestion des comptes	Mots de passe	Modification	Non	Le fournisseur de service doit être en mesure de garantir que les politiques relatives aux mots de passe sont définies pour empêcher les utilisateurs de modifier leurs mots de passe plus souvent que tous les *N* jours, *N* étant spécifié par le propriétaire d'actif.	Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de configurer des politiques relatives aux mots de passe visant à empêcher les utilisateurs de modifier les mots de passe en permanence pour revenir à un mot de passe favori. La période de *N* jours signifie qu'une fois le mot de passe modifié, l'utilisateur est tenu d'attendre *N* jours pour le modifier de nouveau.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.09.09	BR	Gestion des comptes	Mots de passe	Partagé	Non	Le fournisseur de service doit être en mesure de garantir que les comptes dont les mots de passe ont été approuvés par le propriétaire d'actif pour être partagés avec le fournisseur de service sont documentés et gérés en toute sécurité.	Les capacités spécifiées par cette BR et ses RE sont utilisées pour garantir la gestion de l'utilisation des mots de passe partagés. En l'absence d'une gestion des mots de passe partagés, le propriétaire d'actif peut ne pas être informé ou perdre la trace de celui qui a accès à la Solution d'Automatisation. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de gérer et protéger les mots de passe qui lui ont été divulgués par le propriétaire d'actif. Le fournisseur de service est redevable et responsable de la gestion d'un journal sur l'utilisation de chaque compte par son personnel, y compris ses sous-traitants, consultants et représentants.
SP.09.09	RE(1)	Gestion des comptes	Mots de passe	Partagé	Non	Le fournisseur de service doit être en mesure de signaler au propriétaire d'actif les mots de passe qui ont été 1) partagés et qui ne nécessitent plus d'être partagés, 2) délibérément divulgués ou 3) délibérément compromis, et d'aider le propriétaire d'actif à modifier les mots de passe si nécessaire.	Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garder une trace des mots de passe (y compris les mots de passe des comptes de connexion automatique) qui ont été partagés avec le fournisseur de service ou qui sont réputés avoir été compromis ou divulgués à d'autres personnes, et de les signaler au propriétaire d'actif pour qu'ils soient modifiés. Par exemple, le fournisseur de service est tenu de signaler au propriétaire d'actif les mots de passe partagés au sein de son organisation, dès qu'il n'en a plus besoin. Pour modifier ces mots de passe, le propriétaire d'actif peut exiger l'assistance du fournisseur de service. De la même manière, si le personnel du fournisseur de service partage des mots de passe avec d'autres personnes, le fournisseur de service est tenu de signaler ces comptes/mots de passe au propriétaire d'actif lorsqu'il n'est plus utile de les partager. Les mots de passe sont souvent partagés lors des essais, de la mise en service, du dépannage et de la maintenance. De plus, si le fournisseur de service suspecte qu'un mot de passe a été compromis, il convient d'en informer le propriétaire du compte et de demander la modification du mot de passe.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.10.01	BR	Protection contre les logiciels malveillants	Processus manuel	Mécanisme de protection contre les logiciels malveillants	Non	Le fournisseur de service doit être en mesure de fournir au propriétaire d'actif des instructions documentées pour les bonnes installation, configuration et mise à jour des mécanismes de protection contre les logiciels malveillants qui sont soumis à essai et vérifiés pour la Solution d'Automatisation.	La capacité spécifiée par cette BR est utilisée pour garantir que le propriétaire d'actif dispose de la documentation nécessaire pour l'usage des mécanismes de protection contre les logiciels malveillants qui sont compatibles avec la Solution d'Automatisation. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de fournir la documentation relative aux logiciels de protection communément acceptés contre les logiciels malveillants (antivirus, liste blanche, par exemple) fonctionnant sur les plateformes matérielles de la Solution d'Automatisation (stations de travail, par exemple) dont est responsable le fournisseur de service. Si le fournisseur du système de commande ne soumet pas à essai ni ne recommande un produit de protection contre les logiciels malveillants, il est tenu d'être en mesure d'assurer ces fonctions.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.10.02	BR	Protection contre les logiciels malveillants	Outils et logiciels de sécurité	Installation	Non	Le fournisseur de service doit être en mesure de garantir que: 1) les mécanismes de protection contre les logiciels malveillants ont été correctement installés/mis à jour et configurés conformément aux procédures validées du fournisseur de service, 2) les fichiers de définition de logiciel malveillant sont installés pendant la période convenue avec le propriétaire d'actif, 3) les configurations de logiciel malveillant sont gérées et à jour.	Les capacités spécifiées par cette BR et ses RE sont utilisées pour garantir que la Solution d'Automatisation est protégée contre les logiciels malveillants. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant d'installer, de mettre à jour et de configurer un logiciel de protection contre les logiciels malveillants pour la Solution d'Automatisation dont il est responsable. Il s'agit de disposer d'un logiciel de protection contre les logiciels malveillants avec les dernières données, configurations et mises à jour logicielles sur toutes les plateformes matérielles concernées dans la Solution d'Automatisation. Cela signifie également que le fournisseur de service dispose d'un processus identifiable permettant de conclure un accord avec le propriétaire d'actif sur la période entre la publication des fichiers de définition de logiciel malveillant et leur installation. EXEMPLE 1 Si un logiciel antivirus est utilisé, les fichiers de définition d'antivirus sont installés pendant la période convenue. EXEMPLE 2 Si un logiciel de liste blanche est utilisé, les configurations de liste blanche sont maintenues à jour.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.10.02	RE(1)	Protection contre les logiciels malveillants	Outils et logiciels de sécurité	Installation	Non	Le fournisseur de service doit créer et gérer la documentation qui décrit l'utilisation des mécanismes de protection contre les logiciels malveillants dans la Solution d'Automatisation dont est responsable le fournisseur de service. Cette documentation doit inclure, pour chaque composant utilisé dans la Solution d'Automatisation: 1) l'état d'installation des mécanismes de protection contre les logiciels malveillants ou une déclaration selon laquelle il est techniquement impossible d'installer des mécanismes de protection contre les logiciels malveillants sur le composant, 2) les paramètres de configuration en cours du mécanisme installé de protection contre les logiciels malveillants, 3) le statut en cours du fichier de définition de logiciel malveillant dont l'installation sur le composant est approuvée, 4) l'utilisation d'autres fonctions de limitation et de fonctions permettant de réduire le risque d'infection et/ou limiter les effets des infections (isolement des infections, signalement des infections, par exemple).	Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de documenter le statut du logiciel de protection contre les logiciels malveillants pour chaque plateforme matérielle dans la Solution d'Automatisation, que le logiciel de protection contre les logiciels malveillants soit installé ou non sur le composant. Toutes les plateformes nécessitent d'être équipées d'un logiciel de protection contre les logiciels malveillants, sauf si cela n'est pas réalisable d'un point de vue technique (il n'existe aucun logiciel de protection contre les logiciels malveillants, par exemple).

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.10.03	BR	Protection contre les logiciels malveillants	Outils et logiciels de sécurité	Détection	Non	Le fournisseur de service doit être en mesure de vérifier que le logiciel malveillant, sauf le logiciel malveillant de jour zéro, peut être détecté et correctement traité par les mécanismes installés de protection contre les logiciels malveillants.	La capacité spécifiée par cette BR est utilisée pour vérifier que les mécanismes de protection contre les logiciels malveillants fonctionnent comme prévu. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de vérifier qu'un fichier infecté peut être détecté, puis mis en quarantaine/supprimé par le produit de protection contre les logiciels malveillants. La seule exception est l'infection de jour zéro, qui est une infraction pour laquelle aucun fichier de définition de logiciel malveillant n'est disponible. Il s'agit généralement du cas où le logiciel malveillant n'a pas été antérieurement observé ou détecté.
SP.10.04	BR	Protection contre les logiciels malveillants	Processus manuel	Fichiers de définition de logiciel malveillant	Oui	Le fournisseur de service doit être en mesure de fournir au propriétaire d'actif la documentation décrivant: 1) la manière dont sont évalués et approuvés les fichiers de définition de logiciel malveillant pour la Solution d'Automatisation, 2) le signalement au propriétaire d'actif du statut des fichiers de définition de logiciel malveillant *N* jours après la publication des fichiers par le fabricant, *N* ayant été convenu entre le fournisseur de service et le propriétaire d'actif. Ce statut inclut l'applicabilité (le composant et la version, par exemple) et l'état d'approbation (approuvé, installé, désapprouvé, etc.) pour chaque fichier de définition de logiciel malveillant.	La capacité spécifiée par cette BR est utilisée pour garantir que le fournisseur de service dispose d'un processus permettant de vérifier que les nouveaux fichiers de définition de logiciel malveillant sont compatibles avec la Solution d'Automatisation et qu'ils sont disponibles pour la Solution d'Automatisation en temps opportun. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant d'approuver les fichiers de définition de logiciel malveillant, et d'informer le propriétaire d'actif des résultats dans un délai convenu d'un commun accord après leur publication par le fabricant de logiciels de protection contre les logiciels malveillants. Cela n'implique aucune installation dans ce délai, mais seulement que l'installation des fichiers soit approuvée dans ce délai. Le terme "approbation" signifie que le fournisseur de service a évalué les fichiers en conflit avec leur système. Les fichiers en conflit de fonctionnement avec le système ne sont pas approuvés.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.10.05	BR	Protection contre les logiciels malveillants	Appareils – Tous	Nettoyage	Non	Le fournisseur de service doit être en mesure de garantir que tous les appareils, y compris les stations de travail, fournis à la Solution d'Automatisation par le fournisseur de service ne présentent aucun logiciel malveillant connu avant l'utilisation dans la Solution d'Automatisation.	La capacité spécifiée par cette BR est utilisée pour garantir que les appareils contenant des infections détectables ne sont pas installés dans la Solution d'Automatisation. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de vérifier/garantir l'absence de logiciel malveillant dans le matériel qu'il fournit à la Solution d'Automatisation. Il peut s'agir de vérifier l'absence de logiciel malveillant dans le matériel, d'installer le logiciel sur le matériel sur site à partir d'un support exempt de logiciel malveillant (voir SP.10.05 RE(2)) et/ou de garantir que la chaîne logistique fournit des matériels sans logiciel malveillant (le fournisseur du système de commande procède à une analyse de logiciel malveillant avant la livraison, par exemple). Voir l'ISO 27036 pour plus d'informations relatives à la sécurité de la chaîne logistique.
SP.10.05	RE(1)	Protection contre les logiciels malveillants	Support portable	Usage	Non	Le fournisseur de service doit être en mesure de garantir que les supports portables qu'il utilise pour les essais, la mise en service et/ou la maintenance du système sont utilisés à cet effet uniquement.	La capacité spécifiée par cette RE est utilisée pour garantir que les supports portables ne sont pas utilisés à l'extérieur de la Solution d'Automatisation en vue de réduire le risque d'être infectés par des logiciels malveillants. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir qu'il ne fait pas usage des supports portables qu'il utilise à l'appui de la Solution d'Automatisation (qui sont susceptibles d'infecter la Solution d'Automatisation avec des logiciels malveillants) en d'autres lieux où ils pourraient être infectés. Par exemple, si un périphérique de stockage USB contient des outils ou des données de diagnostic, il convient de ne pas le connecter à une station de travail ou un serveur ne faisant pas partie intégrante de la Solution d'Automatisation.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.10.05	RE(2)	Protection contre les logiciels malveillants	Support portable	Nettoyage	Non	Le fournisseur de service doit être en mesure de garantir que les supports portables, y compris les supports d'installation et les ordinateurs portables, utilisés dans ou connectés à la Solution d'Automatisation par le fournisseur de service ne présentent aucun logiciel malveillant connu avant l'utilisation dans la Solution d'Automatisation.	La capacité spécifiée par cette RE est utilisée pour garantir que les supports portables contenant des infections détectables ne sont pas utilisés dans la Solution d'Automatisation. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant d'éviter que des appareils portables infectés ne contaminent la Solution d'Automatisation. Les types de supports portables incluent, sans toutefois s'y limiter: lecteur CD/DVD/ Blu-ray Media, périphériques de stockage USB, téléphones intelligents, mémoire flash, disques électroniques, disques durs et ordinateurs portables. Voir SP.07.XX pour les exigences associées à la connexion à distance à la Solution d'Automatisation.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.11.01	BR	Gestion des correctifs	Processus manuel	Qualification des correctifs	Oui	Le fournisseur de service doit être en mesure de fournir au propriétaire d'actif la documentation décrivant la manière dont les correctifs de sécurité pour le logiciel de la Solution d'Automatisation dont il est responsable sont évalués et approuvés. NOTE 1 Dans la présente norme, les mises à jour de micrologiciels sont considérées comme des correctifs logiciels. NOTE 2 Dans la présente norme, l'installation de correctifs se rapporte à l'installation des correctifs dans la Solution d'Automatisation.	La capacité spécifiée par cette BR est utilisée pour garantir que le fournisseur de service dispose d'un processus documenté qui peut être examiné par le propriétaire d'actif pour vérifier que les nouveaux correctifs de sécurité pour le logiciel sont compatibles avec la Solution d'Automatisation (voir SP.10.04 BR). Dans de nombreux cas, le fournisseur de service utilise la documentation provenant du fournisseur de produit de système de commande et la modifie pour la Solution d'Automatisation, si nécessaire. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de fournir au propriétaire d'actif un document décrivant ses politiques de détermination des correctifs de sécurité qui s'appliquent à la Solution d'Automatisation, et la manière dont ils sont soumis à essai et approuvés. Cela inclut les correctifs de sécurité pour le système de commande et les composants logiciels, les logiciels de système d'exploitation et les applications logicielles des tiers intégrées dans ou avec la Solution d'Automatisation, le système de commande et les composants. L'IEC TR 62443-2-3 décrit la gestion des correctifs et présente un ensemble de responsabilités connexes pour le fournisseur du système de commande et le propriétaire d'actif. SP 11.XX définit les capacités de gestion des correctifs pour le fournisseur de service à l'appui des responsabilités de gestion des correctifs du propriétaire d'actif dans l'IEC TR 62443-2-3.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.11.01	RE(1)	Gestion des correctifs	Processus manuel	Qualification des correctifs	Non	Le fournisseur de service doit être en mesure de revoir, suite aux changements des risques de sécurité, la manière dont il évalue et approuve les correctifs de sécurité pour le logiciel de la Solution d'Automatisation dont il est responsable.	La capacité spécifiée par cette RE est utilisée pour garantir que le fournisseur de service est en mesure de mettre à jour son processus d'évaluation des correctifs en réponse aux évolutions en matière de menaces de cybersécurité (les nouvelles menaces peuvent nécessiter une réponse plus rapide, par exemple). En règle générale, ceci est démontré dans le cadre de ses capacités de gestion des incidents ou d'un processus séparé de revue régulière de son processus d'évaluation des correctifs. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de revoir son processus d'évaluation et d'approbation des correctifs de sécurité. Ces revues sont nécessaires pour pouvoir mettre à jour ce processus et s'adapter aux changements dans le domaine des risques. Il est nécessaire de réaliser cette revue régulièrement ou explicitement en réponse aux changements significatifs dans le domaine des risques. Les changements significatifs sont ceux qui sont réputés avoir un impact potentiel sur le processus. Les changements dans le domaine des risques incluent en général de nouvelles menaces et vulnérabilités, ainsi que le développement de nouvelles technologies de sécurité.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.11.02	BR	Gestion des correctifs	Liste des correctifs	Qualification des correctifs	Oui	Le fournisseur de service doit être en mesure de mettre à la disposition du propriétaire d'actif la documentation décrivant les correctifs/mises à jour de sécurité. La description de chaque correctif doit être mise à disposition du propriétaire d'actif dans un délai convenu après la publication d'un correctif par son fabricant, et doit inclure: 1) les correctifs de sécurité applicables aux composants de la Solution d'Automatisation dont le fournisseur de service est responsable, 2) le statut d'approbation/état du cycle de vie (voir IEC TR 62443-2-3) de chacun d'eux, c'est-à-dire approuvé, refusé, non applicable, en essai 3) un avertissement indiquant si l'application d'un correctif approuvé requiert ou génère un redémarrage du système 4) la raison du refus d'approbation ou d'application, 5) un plan de correction pour ceux qui sont applicables, mais pas approuvés.	Les capacités spécifiées par cette BR et ses RE sont utilisées par le propriétaire d'actif pour accéder aux descriptions des correctifs de sécurité qui sont pertinents pour la Solution d'Automatisation du fournisseur de service et pour inciter ce dernier à recommander une méthode de limitation des vulnérabilités pour les correctifs que le propriétaire d'actif choisit de ne pas installer. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant d'évaluer et d'approuver les correctifs de sécurité tel que cela est documenté par la capacité définie dans SP.11.01 BR, et d'informer le propriétaire d'actif des résultats dans les *N* jours qui suivent la publication du correctif par son fabricant, *N* étant convenu entre le fournisseur de service et le propriétaire d'actif. Le fournisseur de service peut utiliser des bibliothèques de logiciels améliorées ou différentes de celles fournies par le ou les fabricants. Dans ce cas, le fournisseur de service peut devoir modifier un module de correctif logiciel. Ce type de question est à aborder dans le cadre de cette exigence.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.11.02	RE(1)	Gestion des correctifs	Liste des correctifs	Qualification des correctifs	Non	Le fournisseur de service doit être en mesure de mettre à la disposition du propriétaire d'actif, par l'intermédiaire d'une interface communément acceptée par les communautés industrielles et de sécurité, une liste de correctifs qui identifie: 1) les correctifs de sécurité approuvés applicables au logiciel de la Solution d'Automatisation dont le fournisseur de service est responsable (logiciel de système de commande et de composant, logiciel de système d'exploitation et applications logicielles de tiers, par exemple), 2) les correctifs de sécurité applicables dont l'utilisation dans la Solution d'Automatisation a été approuvée, 3) les numéros de version du logiciel auxquels s'appliquent les correctifs approuvés. La liste doit être mise à disposition du propriétaire d'actif dans un délai convenu après la publication d'un correctif par son fabricant.	Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de décrire au propriétaire d'actif la manière de récupérer par voie électronique, une liste décrivant les correctifs de sécurité approuvés qui sont applicables aux composants dont le fournisseur de service est responsable (voir SP.11.02 BR). Cette liste est à fournir par l'intermédiaire d'une interface communément acceptée permettant au propriétaire d'actif de prendre connaissance des correctifs à télécharger auprès du fabricant ou d'autres moyens de les obtenir. Cette liste peut être récupérée par l'intermédiaire de cette interface auprès du fournisseur de produit de système de commande, du fournisseur de service ou d'un autre agent identifié par le fournisseur de service. NOTE Le terme "approuvé" est censé impliquer que les correctifs ont été soumis à essai et validés par le fournisseur de service selon une configuration connue et qu'aucun problème n'a été détecté.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.11.02	RE(2)	Gestion des correctifs	Liste des correctifs	Approbation	Non	Le fournisseur de service doit être en mesure de: 1) recommander un plan d'atténuation à la demande du propriétaire d'actif pour les correctifs de sécurité qui ont été appliqués et approuvés par le fournisseur de service, mais qui n'ont pas été approuvés par le propriétaire d'actif, du fait par exemple de leur éventuel impact sur les opérations ou les performances (voir SP 11.05 BR), 2) mettre en œuvre le plan d'atténuation après approbation du fournisseur d'actif.	Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de développer et de mettre en œuvre une approche pour atténuer l'impact de n'être pas autorisé à installer un correctif de sécurité susceptible d'affecter la Solution d'Automatisation. Cette approche peut inclure des mécanismes de compensation ou d'autres moyens de réduire les vulnérabilités traitées par le correctif de sécurité. Les autres approches sont soumises à l'approbation du propriétaire d'actif.
SP.11.03	BR	Gestion des correctifs	Correctif de sécurité	Livraison	Non	La gestion des correctifs par le fournisseur de service doit assurer: 1) l'obtention des correctifs par le propriétaire d'actif directement auprès du fabricant et/ou 2) la redistribution des correctifs par le fournisseur de service uniquement si elle a été approuvée par le propriétaire d'actif et autorisée par le fabricant de correctifs.	La capacité spécifiée par cette BR est utilisée pour garantir que les correctifs sont obtenus par l'intermédiaire d'un canal autorisé (auprès d'une source appropriée) pour réduire la possibilité d'être non valides/infectés. Cela signifie que la politique de livraison de correctif du fournisseur de service implique l'obtention par le propriétaire d'actif du correctif directement auprès du fabricant de correctifs, ou auprès du fournisseur de service à la demande du propriétaire d'actif, et puis uniquement si les contrats de licence avec le fabricant de correctifs le permettent. Si les correctifs sont à livrer par le fournisseur de service, ce dernier et le propriétaire d'actif sont tenus de décider en commun de la méthode de livraison (DVD, connexion sécurisée, par exemple).

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.11.04	BR	Gestion des correctifs	Correctif de sécurité	Installation	Oui	Le fournisseur de service doit être en mesure de fournir la documentation au propriétaire d'actif, indiquant comment exécuter le correctif manuellement et par l'intermédiaire d'un serveur de gestion de correctifs, et comment obtenir les rapports d'état de correctif. 1) Lors de l'utilisation d'un serveur de gestion de correctifs, la documentation doit être fournie pour expliquer son utilisation pour installer les correctifs 2) Pour l'application manuelle des correctifs à l'aide d'un support portable, la documentation doit être fournie pour expliquer comment installer les correctifs à partir du support.	La capacité spécifiée par cette BR est utilisée pour garantir que le propriétaire d'actif a connaissance de la méthode d'installation des correctifs de sécurité pour la Solution d'Automatisation. Cela signifie que le fournisseur de service est en mesure de fournir les instructions au propriétaire d'actif décrivant la méthode d'installation des correctifs à partir d'un support portable (CD, DVD, périphériques de stockage USB) et d'un serveur de gestion de correctifs.
SP.11.05	BR	Gestion des correctifs	Correctif de sécurité	Approbation	Non	Le fournisseur de service doit être en mesure de garantir qu'il obtient l'approbation du propriétaire d'actif pour l'installation de chacun et de l'ensemble des correctifs de sécurité.	La capacité spécifiée par cette BR est utilisée pour garantir que le fournisseur de service installe des correctifs si et uniquement si le propriétaire d'actif veut qu'ils soient installés. Cela signifie que le fournisseur de service dispose d'une politique l'obligeant à obtenir l'approbation du propriétaire d'actif pour l'installation des correctifs.
SP.11.06	BR	Gestion des correctifs	Correctif de sécurité	Installation	Non	Le fournisseur de service doit être en mesure de garantir que si le propriétaire d'actif demande au fournisseur de service d'installer des correctifs logiciels de sécurité (y compris les mises à jour de micrologiciels), le fournisseur de service les installe dans un délai spécifié par le propriétaire d'actif.	La capacité spécifiée par cette BR est utilisée pour garantir que le fournisseur de service installe des correctifs uniquement lorsque le propriétaire d'actif veut qu'ils soient installés, par exemple, pour éviter la perturbation du processus s'il faut qu'un appareil redémarre après l'installation. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant d'installer des correctifs approuvés seulement dans un délai spécifié par le propriétaire d'actif.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.11.06	RE(1)	Gestion des correctifs	Correctif de sécurité	Installation	Non	Le fournisseur de service doit être en mesure de garantir que le niveau de renforcement de la sécurité de la Solution d'Automatisation est maintenu après l'installation du correctif, en réinstallant le logiciel ou en modifiant les paramètres de configuration du système, par exemple	La capacité spécifiée par cette RE est utilisée pour garantir que l'installation du correctif "n'annule" pas ni ne dégrade le renforcement de la Solution d'Automatisation. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir qu'il a un processus de restauration de l'état de renforcement de la Solution d'Automatisation si l'installation du correctif occasionne la dégradation de cet état. Cette capacité ne dépend pas de celui qui installe les correctifs. Il n'est pas rare que l'installation de correctifs et de mises à jour du système exige ou restaure automatiquement des paramètres de configuration qui suppriment ou dégradent le renforcement du système (l'installation d'un Service Pack de Microsoft, par exemple). Par conséquent, le fournisseur de service est tenu de disposer d'un processus permettant de déterminer si cela s'est produit, et s'il faut restaurer le renforcement.
SP.11.06	RE(2)	Gestion des correctifs	Correctif de sécurité	Installation	Non	Le fournisseur de service doit être en mesure de garantir que, pour les appareils prenant en charge l'installation de logiciels/micrologiciels sur le réseau, le processus de mise à jour garantit l'authenticité et l'intégrité du logiciel/micrologiciel de l'appareil.	La capacité spécifiée par cette RE est utilisée pour garantir que les correctifs installés sur le réseau sont authentiques et ne sont pas corrompus au cours du processus d'application de correctifs. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de mettre à jour en toute sécurité le logiciel/micrologiciel dans les appareils. Il s'agit de permettre uniquement aux utilisateurs autorisés de procéder aux mises à jour, et de s'assurer que l'image de la mise à jour envoyée à l'appareil est protégée contre les modifications lors de sa transmission. L'application des correctifs peut exposer des images de logiciels au réseau. Voir SP.03.10 BR et ses RE pour la protection des données sensibles. Voir l'IEC 62443-3-3 et l'IEC 62443-4-2 pour les exigences relatives à l'authentification, l'autorisation, l'intégrité et la confidentialité.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.11.06	RE(3)	Gestion des correctifs	Correctif de sécurité	Installation	Non	Le fournisseur de service doit être en mesure de déterminer l'état d'installation de tous les correctifs de sécurité applicables à la Solution d'Automatisation dont il est responsable.	Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de savoir si les correctifs approuvés pour la Solution d'Automatisation ont été installés en vue de déterminer les correctifs qui manquent (ne sont pas installés). Cette capacité peut être fournie avec des procédures manuelles ou des outils automatisés.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.12.01	BR	Sauvegarde/ Restauration	Processus manuel	Description technique	Oui	Le fournisseur de service doit être en mesure de fournir la documentation pour les procédures de sauvegarde recommandées pour la Solution d'Automatisation, y compris ce qui suit, sans toutefois s'y limiter: 1) Instructions sur la manière de procéder à une sauvegarde complète de la Solution d'Automatisation et des sauvegardes partielles, le cas échéant, à l'aide d'au moins l'une des méthodes suivantes a) architecture de sauvegarde propriétaire sur des supports amovibles, b) architecture de sauvegarde de système simple sur des supports amovibles c) architecture de sauvegarde distribuée dans laquelle chaque système de sauvegarde conserve un sous-ensemble des Solutions d'Automatisation du fournisseur de service sur le site du propriétaire d'actif, ou d) architecture de sauvegarde centralisée utilisant un système de sauvegarde pour toutes les Solutions d'Automatisation du fournisseur de service sur le site du propriétaire d'actif 2) Dispositions pour la sauvegarde des types de données suivants a) fichiers de système d'exploitation et données cryptographiques (élément de mise à la clé, par exemple), b) applications (y compris les intergiciels tels que les logiciels de tunnellisation),	La capacité spécifiée par cette BR garantit que le propriétaire d'actif sait comment utiliser les capacités de sauvegarde fournies par le fournisseur de service pour la Solution d'Automatisation. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de préparer un document spécifique à la Solution d'Automatisation, qui définit la manière de sauvegarder la Solution d'Automatisation, détermine les données à sauvegarder dans le cadre de sauvegardes complètes ou partielles, et la manière dont il recommande de gérer le stockage hors site. Il convient que cette documentation reconnaisse que: 1) l'image de sauvegarde est considérée comme étant sensible (voir SP.03.10 BR et ses RE pour la protection des données sensibles) et peut par conséquent être une cible pour les failles de sécurité. 2) la sauvegarde peut être nécessaire pour la reprise après incidents de sécurité (la corruption d'une station de travail, par exemple). 3) le propriétaire d'actif peut disposer d'une stratégie de sauvegarde généralement dépendante d'exigences commerciales. 4) la stratégie de sauvegarde du propriétaire d'actif peut inclure des sujets relatifs à la fréquence de sauvegarde, aux sauvegardes partielles, au moment où il convient de faire des sauvegardes (par exemple, avant les modifications techniques) et à la reprise après infection qui peut influencer le contenu de la documentation du fournisseur de service. 5) Il convient de terminer la sauvegarde avant de procéder à des modifications susceptibles de l'interrompre ou de générer des incohérences dans les données de sauvegarde. Il s'agit, par exemple, de modifications techniques et de l'installation de correctifs.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
						c) données de configuration, fichiers de base de données, d) journaux, journal électronique, e) types de fichiers non conventionnels, y compris, sans toutefois s'y limiter, les paramètres des équipements de réseau, les paramètres de contrôleur de système de commande (paramètres de réglage, points de consigne, niveaux d'alarme), f) paramètres d'appareillage de terrain, et g) informations du répertoire h) autres fichiers identifiés par le fournisseur de service exigés pour la création d'une sauvegarde complète de la Solution d'Automatisation. 3) Recommandations pour le stockage hors site des supports de sauvegarde 4) Dispositions pour garantir que les modifications à la Solution d'Automatisation pendant une sauvegarde susceptibles de compromettre l'intégrité d'une sauvegarde ne sont pas apportées. NOTE Des exemples de restaurations partielles incluent le système d'exploitation, les logiciels d'application, les bases de données et les fichiers de configuration.	

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.12.02	BR	Sauvegarde/ Restauration	Restauration	Description technique	Oui	Le fournisseur de service doit être en mesure de fournir au propriétaire d'actif des instructions documentées pour le rétablissement du fonctionnement normal de la Solution d'Automatisation ou de ses composants.	La capacité spécifiée par cette BR garantit que le propriétaire d'actif sait comment utiliser les capacités de restauration fournies par le fournisseur de service pour la Solution d'Automatisation. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant d'élaborer ou de fournir la documentation décrivant la manière de restaurer la Solution ou ses composants (c'est-à-dire une restauration partielle) à partir de données de sauvegarde. Il convient que la documentation comporte des instructions de traitement des scénarii anormaux (la restauration d'une Solution d'Automatisation dont l'architecture peut avoir été modifiée depuis la dernière sauvegarde, par exemple). Dans ces cas, la restauration peut ne pas être complète, et il convient d'informer le propriétaire d'actif de l'éventuelle occurrence de ce type de condition. Cette exigence s'applique aux Solutions d'Automatisation opérationnelles et aux simulations.
SP.12.03	BR	Sauvegarde/ Restauration	Support portable	Description technique	Oui	Le fournisseur de service doit être en mesure de fournir au propriétaire d'actif la documentation décrivant la manière de contrôler et de gérer en toute sécurité les supports de sauvegarde amovibles.	La capacité spécifiée par cette BR garantit que le propriétaire d'actif sait comment traiter en toute sécurité les supports de sauvegarde pour la Solution d'Automatisation. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant d'élaborer un document spécifique à la Solution d'Automatisation, qui décrit le traitement des données de sauvegarde visant à les protéger de manière adaptée en cohérence avec les politiques ou procédures du propriétaire d'actif ou de leurs extensions. Les données de sauvegarde peuvent être une cible pour les failles de sécurité, par exemple, pour empêcher la restauration correcte ou l'accès aux données confidentielles.
SP.12.04	BR	Sauvegarde/ Restauration	Sauvegarde	Vérification	Oui	Le fournisseur de service doit être en mesure de fournir au propriétaire d'actif la documentation décrivant la manière de vérifier la réussite de la sauvegarde du système.	La capacité spécifiée par cette BR garantit que le propriétaire d'actif sait comment vérifier la sauvegarde pour la Solution d'Automatisation. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant d'élaborer (ou de fournir) un document qui décrit comment vérifier la réussite de la sauvegarde.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.12.05	BR	Sauvegarde/ Restauration	Restauration	Vérification	Non	Le fournisseur de service doit être en mesure de vérifier: 1) qu'il est possible de procéder à une sauvegarde complète de la Solution d'Automatisation, et 2) qu'il est possible de restaurer une Solution d'Automatisation en total état de fonctionnement à partir de cette sauvegarde.	La capacité spécifiée par cette BR garantit que les capacités de sauvegarde et de restauration au profit de la Solution d'Automatisation fonctionnent comme prévu. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de démontrer, voire de vérifier, qu'une sauvegarde peut aboutir et que la Solution d'Automatisation peut être restaurée à partir de cette sauvegarde. Il convient que ce processus soit assez souple pour permettre au propriétaire d'actif de demander uniquement une sauvegarde/restauration partielle pour s'assurer que la capacité de sauvegarde peut être utilisée avec succès. Si la sauvegarde inclut des bases de données, cela signifie également que le fournisseur de service dispose d'un processus identifiable permettant de démontrer, voire de vérifier, que l'annulation automatique est arrêtée/désactivée avant de lancer la sauvegarde. L'annulation automatique peut générer des incohérences dans la base de données, si elle a lieu pendant la sauvegarde de la base de données.
SP.12.06	BR	Sauvegarde/ Restauration	Sauvegarde	Réalisation	Non	Le fournisseur de service doit être en mesure de réaliser la sauvegarde de la Solution d'Automatisation conformément aux programmes de sauvegarde et aux objectifs de restauration des données et de reprise après sinistre du propriétaire d'actif.	La capacité spécifiée par cette BR garantit que, lors de la sauvegarde de la Solution d'Automatisation, le fournisseur de service respecte les lignes directrices/politiques du propriétaire d'actif. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de respecter les stratégies et objectifs du propriétaire d'actif en matière de sauvegarde/restauration, y compris les programmes de sauvegarde et les plans de reprise après sinistre (voir SP.12.09 BR). Cette exigence a pour objet de s'assurer que le fournisseur de service est prêt à intégrer ses activités de sauvegarde/restauration aux exigences de sauvegarde du propriétaire d'actif.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.12.07	BR	Sauvegarde/ Restauration	Sauvegarde	Robustesse	Non	Le fournisseur de service doit être en mesure de garantir que la Solution d'Automatisation peut continuer à fonctionner normalement pendant une sauvegarde.	La capacité spécifiée par cette BR garantit que le processus de sauvegarde n'affecte pas le fonctionnement de la Solution d'Automatisation (le contrôle du processus, par exemple). Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant de garantir que les opérations de sauvegarde ne gênent pas le fonctionnement normal de la Solution d'Automatisation. Pour les exigences connexes de capacité du système, voir l'IEC 62443-3-3.
SP.12.08	BR	Sauvegarde/ Restauration	Processus manuel	Journalisation	Oui	Le fournisseur de service doit être en mesure de fournir au propriétaire d'actif la documentation décrivant la manière de générer et gérer les journaux d'audit de toutes les activités de sauvegarde et de restauration.	La capacité spécifiée par cette BR garantit que le propriétaire d'actif sait comment gérer les journaux d'audit pour les opérations de sauvegarde et de restauration. Ces journaux d'audit donnent la preuve des activités de sauvegarde/restauration, en ce qui concerne le moment où elles ont été effectuées, la personne qui les a effectuées et leur statut. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant d'élaborer ou de fournir la documentation décrivant la manière de configurer la Solution d'Automatisation pour écrire des actions de sauvegarde et de restauration dans un journal d'audit.

Tableau A.1 *(suite)*

ID Req	BR/RE	Zone fonctionnelle	Sujet	Sous-sujet	Doc?	Description de l'exigence	Justification
SP.12.09	BR	Sauvegarde/ Restauration	Processus manuel	Reprise après sinistre	Oui	Le fournisseur de service doit être en mesure de documenter le plan recommandé de reprise après sinistre incluant ce qui suit, sans toutefois s'y limiter: 1) Description des différents scénarii de sinistre et leur impact sur la Solution d'Automatisation, 2) Instructions pas-à-pas pour la restauration et le redémarrage des composants ayant fait l'objet d'une défaillance, et leur intégration dans la Solution d'Automatisation, 3) Exigences d'architecture minimales pour la restauration de l'ensemble de la Solution d'Automatisation.	La capacité spécifiée par cette BR garantit qu'il existe non seulement un plan de reprise après sinistre, mais aussi des informations sur les manières possibles de survenance d'un sinistre (y compris les menaces de cybersécurité, par exemple) et le mode de reprise après le sinistre. Cela signifie que le fournisseur de service dispose d'un processus identifiable permettant d'élaborer un document spécifique à la Solution d'Automatisation, qui définit la manière de gérer une crise majeure en fonction d'un scénario de cybersécurité pour la restauration de la Solution d'Automatisation et de ses composants. La sauvegarde et les moyens de restauration ne peuvent pas être compromis par la perte de composants de la Solution d'Automatisation ou de l'ensemble de la Solution d'Automatisation. Les moyens de restauration peuvent inclure les équipements tels qu'un banc d'essai ou des outils de développement autonomes.

Bibliographie

NOTE Cette bibliographie inclut des références aux sources utilisées pour l'élaboration de la présente norme, ainsi que des références aux sources qui peuvent aider le lecteur à mieux appréhender la cybersécurité dans son ensemble et le processus de développement d'un système de gestion de la cybersécurité. Le texte de la présente norme ne mentionne pas toutes les références de cette bibliographie.

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* (disponible en anglais seulement)

ISO/IEC 30111, *Information technology – Security techniques – Vulnerability handling processes* (disponible en anglais seulement)

IEC 61508 (toutes les parties), *Sécurité fonctionnelle des systèmes électriques / électroniques/électroniques programmables relatifs à la sécurité*

IEC 61511 (toutes les parties), *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation*

IEC 62264-1:2013, *Intégration des systèmes entreprise-contrôle – Partie 1: Modèles et terminologie*

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

IEC/TS 62443-1-1, *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models* (disponible en anglais seulement)

IEC/TR 62443-1-2, *Industrial communication networks – Network and system security – Part 1-2: Master glossary of terms and abbreviations* (disponible en anglais seulement) *1*

IEC/TR 62443-1-3, *Industrial communication networks – Network and system security – Part 1-3: System security compliance metrics* (disponible en anglais seulement) *2*

IEC 62443-2-1:2010, *Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes – Partie 2-1: Établissement d'un programme de sécurité pour les systèmes d'automatisation et de commande industrielles*

IEC/TR 62443-2-3, *Industrial communication networks – Network and system security – Part 2-3: Patch management in the IACS environment* (disponible en anglais seulement) *3*

IEC 62443-3-2, *Industrial communication networks – Network and system security – Part 3-2: Security assurance levels for zones and conduits* (disponible en anglais seulement) *4*

_____

1 À l'étude.

2 En cours d'élaboration.

3 En cours d'élaboration.

IEC 62443-3-3:2013, *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels* (disponible en anglais seulement)

IEC 62443-4-1, *Industrial communication networks – Network and system security – Part 4-1: Product development requirements* (disponible en anglais seulement)[5]

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

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

_____

4 En cours d'élaboration.

5 À l'étude.

6 À l'étude.

7 À l'étude.

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