IEC 62443-2-4

Edition 1.0 2017-08

INTERNATIONAL STANDARD

colour
inside

AMENDMENT 1

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

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

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

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

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

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

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

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 It also gives information on projects, replaced and withdrawn publications.

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

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

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

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

IEC 62443-2-4

Edition 1.0 2017-08

INTERNATIONAL STANDARD

colour inside

AMENDMENT 1

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 25.040.40; 35.110

ISBN 978-2-8322-4366-4

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

FOREWORD

This amendment has been prepared by IEC technical committee 65: Industrial-process measurement, control and automation.

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

CDV	Report on voting
65/637A/CDV	65/661/RVC

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

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.

1 Scope

Replace the first paragraph by the following new text:

This part of IEC 62443 specifies a comprehensive set of requirements for security capabilities for IACS service providers that they can offer to the asset owner during integration and maintenance activities of an Automation Solution. Because not all requirements apply to all industry groups and organizations, Subclause 4.1.4 provides for the development of Profiles that allow for the subsetting of these requirements. Profiles are used to adapt this document to specific environments, including environments not based on an IACS.

Delete Note 4 and renumber Note 5 to "Note 4"*.*

3.1.14
safety instrumented system

Add the following Note 2 to entry:

Note 2 to entry: Not all industry sectors use this term. This term is not restricted to any specific industry sector, and it is used generically to refer to systems that enforce functional safety. Other equivalent terms include safety systems and safety related systems.

4.1.4 Profiles

Replace the existing text with the following:

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

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

Each TR may define one or more profiles, and each profile identifies a subset of the requirements defined in Annex A and specifies, where necessary, how specific requirements are to be applied in the environment where they are to be used.

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

4.2 Maturity model

Table 1 – Maturity levels

Replace, in the fourth column, row for Level 2, the second paragraph that begins with “At this level, the service provider has…” *by the following:*

At this level, the service provider has the capability to manage the delivery and performance of the service according to written policies (including objectives). The service provider also has evidence to show that personnel who will perform the service have the expertise, are trained, and/or are capable of following written procedures to perform the service.

5.1 Contents

Insert the following new paragraph between the first paragraph and the note:

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

5.3 IEC 62264-1 hierarchy model

Replace the first paragraph with the following:

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

5.5.3 Functional area column

Replace the first paragraph with the following:

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

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

5.5.7 Requirement description

Add “column” *to the title as follows:*

Requirement description column

Replace the existing text with the following:

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

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

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

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

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

5.5.8 Rationale

Add “column” *to the title as follows:*

Rationale column

Annex A – Security requirements

Table A.1 – Security program requirements

Change the text in the "Requirement description" *and* "Rationale" *columns to:*

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

Change the text in the “Requirement description” *and* “Rationale” *columns to:*

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, where feasible, and to the extent allowed by applicable law.	Having this capability means that the service provider has an identifiable process for verifying the integrity of the subcontractors, consultants, and representatives of the service provider who will be assigned to work on the Automation Solution. This requirement also recognizes that the ability to perform background checks is not always possible because of applicable laws or because of lack of support by local authorities and/or service organizations. For example, there may be countries that do not prohibit background checks, but that provide no support for conducting a background check, making it infeasible or impractical for the service provider to perform such a check. How and how often background checks are performed are left to the service provider. Examples of background checks include identity verification and criminal record checks. See ISO/IEC 27036-3 for additional supply chain organizational requirements.

Change the text in the “Requirement description” *and* “Rationale” *columns to:*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc ?	Requirement description	Rationale
SP.01.06	BR	Solution staffing	Personnel assignments	Security lead	No	The service provider shall have documented minimum IACS cyber-security qualifications for security lead positions and the capability to assign security leads to Automation Solutions who meet these qualifications.	The capability specified by this BR is used to reduce errors in security decision making and implementation. Making poor choices or lacking the ability to properly implement security can unnecessarily expose the Automation Solution to security threats and/or compromises. Having this capability means that the service provider has documented the qualifications (expertise/competencies) that it requires of personnel who lead cyber-security related activities and has an identifiable process for staffing each Automation Solution with personnel who have this expertise. Expertise may include IACS cyber-security experience, training and certifications, and in general, the service provider and asset owner will typically come to agreement on the cyber-security qualifications for personnel before staffing begins. The phrase "meet these qualifications" is used to indicate that the security leads assigned to the Automation Solution have relevant experiences that confirm their compliance with these qualifications.

Change the text in the “Rationale” *column to:*

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

Change the text in the “Rationale” *column to:*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc ?	Requirement description	Rationale
SP.03.10	RE(2)	Architecture	Data protection	Data/event retention	Yes	The service provider shall have the capability to provide documentation to the asset owner that describes the retention capabilities provided by the Automation Solution for storing/archiving sensitive data. This documentation includes capacities, pruning and purging functions, retention timeouts, etc.	Having this capability means that the service provider has an identifiable process for documenting how the Automation Solution stores/archives sensitive data, such as historical data and events. This may include internal capabilities of the Automation Solution (e.g. data volumes/capacities) or may identify capabilities required to export historical data/events to a history archive. Historical data and events can be used during forensics and event analysis and correlation.

Change the text in the “Requirement description” *and* “Rationale” *columns to:*

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

Change the text in the “Requirement description” *and* “Rationale” *columns to:*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc ?	Requirement description	Rationale
SP.05.03	BR	SIS	Network design	Communications	No	The service provider shall have the capability to ensure that communications external to the Automation Solution, including remote access communications, are not able to interfere with the operation of the SIS.	The capability specified by this BR is used to ensure that the operation of the SIS cannot be impacted by communications of devices/applications external to the Automation Solution. SP.05.02 BR requires capabilities to protect SIS communications from other Automation Solution communications, while this requirement requires capabilities to protect the operation of the SIS from communications external to the Automation Solution. Having this capability means that the service provider has an identifiable process for ensuring that the operation of the SIS cannot be affected by communications of external applications, including remote access communications such as RDP.

Change the text in the “Requirement description” *and* “Rationale” *columns to:*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc ?	Requirement description	Rationale
SP.05.04	BR	SIS	Network design	Communications	No	The service provider shall have the capability to ensure that applications, (e.g. control system applications) external to the SIS are not able to participate in or disrupt or otherwise interfere with SIS communications that are critical to safety functions.	The capability specified by this BR is used to ensure that the SIS cannot be impacted by devices/applications external to the SIS. SP.05.03 BR requires capabilities to protect the SIS from communications external to the Automation Solution, while this requirement requires capabilities to protect SIS communications from interference by applications external to the SIS. Having this capability means that the service provider has an identifiable process for ensuring that there are no communications critical to safety functions (e.g. data and/or commands) transferred between the SIS and applications residing external to the SIS. This requirement is intended to prevent the SIS functions critical to safety operations from being compromised by traffic originating from sources outside the SIS.

Change the text in in the “Requirement description” *and* “Rationale” *columns to:*

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 SIS EWSs that reside outside the SIS (external to SIS interface with the control system) cannot be compromised by communications from Level 3 or above. NOTE The term "Level" refers to the position in the Purdue Reference Model as standardized by ISA 95 and IEC 62264-1 (see 5.3).	The capability specified by this BR is used to employ safeguards, such as network security devices, to ensure that only authorized communications from Level 3 applications to SIS engineering workstations residing outside the SIS are permitted. Access from Level 3 applications to SIS engineering workstations that reside within the SIS is prohibited by SP.05.03 BR. Having this capability means that the service provider has an identifiable process for ensuring that all communications between the SIS engineering workstation and Level 3 (and above) applications pass through a network security device, or equivalent mechanism, that connects Level 2 and Level 3 (or above).

Change the text in the “Requirement description” *and* “Rationale” *columns to:*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc ?	Requirement description	Rationale
SP.05.05	RE(1)	SIS	Devices - Workstations	Communications	No	The service provider shall have the capability to ensure that the Automation Solution's SIS EWSs that reside within the SIS (internal to SIS interface with the control system) cannot be compromised by remote access (e.g. RDP).	The capability specified by this RE is defined to be able to protect SIS engineering workstations that reside inside the SIS from being exploited via remote access connections. See SP.05.05 BR that addresses access from Level 3 to SIS EWSs external to the SIS. Having this capability means that the service provider has an identifiable process for ensuring that SIS engineering workstations within the SIS (1a) either do not have remote access installed or (1b) have it disabled (not accessible), and/or (2) have security mechanisms that block remote access communications with these workstations. NOTE See IEC 62443-3-2 for guidance on what to consider in such risk assessments from a cyber-security perspective.

Change the text in the "Requirement description" *and* "Rationale" *columns to:*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc ?	Requirement description	Rationale
SP.05.06	BR	SIS	Devices - Workstations	Connectivity	No	The service provider shall have the capability to ensure that all access to the Automation Solution's SIS from outside the SIS is mediated and authorized at the interface to the SIS.	The capability specified by this BR is used to limit the number of physical access paths to the SIS, and hence reduce its attack surface. Having this capability means that the service provider has an identifiable process for ensuring that access controls to the SIS are implemented at the interface to the SIS, for example by a gateway used only to provide access to the SIS from the BPCS. Implementation of this gateway may be provided by the BPCS or the SIS.

Change the text in the "Requirement description" *and* "Rationale" *columns to:*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc ?	Requirement description	Rationale
SP.05.07	BR	SIS	Devices - Workstations	Least functionality	No	The service provider shall have the capability to ensure that SIS functions performed by the Automation Solution's SIS EWS are protected from compromise by other SIS EWS software.	The capability specified by this BR is used to reduce the possibility that the SIS EWS will contain T3 offline software (see IEC 61508-3) that could intentionally or inadvertently cause harm to the SIS. Having this capability means that the service provider has an identifiable process for ensuring that safety-related software running in SIS EWSs is protected from compromise from other software running in the SIS EWS.

Change the text in the “Requirement description” *and* “Rationale” *columns to:*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc ?	Requirement description	Rationale
SP.05.08	BR	SIS	Devices - Wireless	Connectivity	No	The service provider shall have the capability to verify that unauthorized wireless devices are not used as an integral part of SIS safety functions.	The capability specified by this BR is used to prevent attacks against the SIS by unauthorized wireless devices. Since wireless devices are not bounded by physical security perimeters nor by physical implementation, they can present a threat to the SIS. Having this capability means that the service provider has an identifiable process for verifying that wireless device communications are not used as an integral part of SIS safety functions when prohibited by the asset owner. “Integral part” refers to communications that are implemented and incorporated into SIS safety functions. See SP.04.01 BR for requirements for the general use of wireless technologies within the Automation Solution.

Change the text in the “Requirement description” *column to:*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc ?	Requirement description	Rationale
SP.05.09	BR	SIS	User interface	Configuration mode	No	The service provider shall have the capability to ensure that SIS configuration mode can be enabled and disabled. While disabled, this interface shall prohibit the SIS from being configured. NOTE This interface will typically prevent configuration messages from being delivered to the SIS.	The capabilities specified by this BR and its REs are used to prevent configuration access to the SIS during normal operation through a mechanism that requires the SIS to be unlocked to configure it, and locked at all other times. Having this capability means that the service provider is able to ensure that the SIS can be locked to prevent configuration changes from being made and unlocked to allow them to be made. Locks can be physical key switches or software controlled locks, but however implemented they allow the SIS to be locked to prevent inadvertent or malicious changes from being made.

Change the text in the “Requirement description” *column to:*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc ?	Requirement description	Rationale
SP.05.09	RE(1)	SIS	User interface	Configuration mode	No	The service provider shall have the capability to provide a hardware implementation of the configuration mode interface required by SP.05.09 BR and to ensure that this hardware implementation is capable of being physically locked while configuration mode is disabled.	The capability specified by this RE is defined to require intentional human intervention to enable configuration of the SIS, such as holding a physical key open (unlocked) while the configuration is being changed, for the purpose of increasing confidence that inadvertent changes to the SIS configuration cannot occur. Having this capability means that the service provider is able to ensure that the SIS has a hardware interface that can be disabled to prevent configuration changes from being made. The hardware interface, such as a physical key switch, when physically locked (e.g. removing the key), configuration mode is disabled.

Change the text in the “Doc?”, “Requirement description” *and* “Rationale” *columns to:*

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

Change the text in the “Rationale” *column to:*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc ?	Requirement description	Rationale
SP.09.09	BR	Account management	Passwords	Shared	No	The service provider shall have the capability to ensure that accounts whose passwords have been approved by the asset owner to be shared with the service provider are securely documented and maintained.	The capabilities specified by this BR and its RE are used to ensure that the use of shared passwords is managed. Without management of shared passwords, the asset owner may not be aware of or lose track of who has access to the Automation Solution. Having this capability means that the service provider has an identifiable process for documenting the list of accounts for which passwords have been divulged to it by the asset owner and protecting that list from unauthorized disclosure and modification. The service provider is accountable and responsible for maintaining a log of who has been given passwords for these accounts, including its subcontractors, consultants, and representatives.

Change the text in the "Rationale" *column to:*

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

Change the text in the “Rationale” *column to:*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc ?	Requirement description	Rationale
SP.10.05	BR	Malware protection	Devices - All	Sanitizing	No	The service provider shall have the capability to ensure that all devices, including workstations, supplied to the Automation Solution by the service provider are free of known malware prior to use in the Automation Solution.	The capability specified by this BR is used to ensure that devices with detectable infections are not installed in the Automation Solution. The term “known malware” is used to indicate malware that has been previously discovered and for which malware definition files have been developed and are available. Having this capability means that the service provider has an identifiable process for verifying/ensuring that malware is not present in equipment provided by it to the Automation Solution. Verification can include checking the equipment for malware, installing software to the equipment at the site from malware-free media (see SP.10.05 RE(2)), and/or ensuring the supply chain provides malware free equipment (e.g. the control system vendor performs malware scans prior to delivery). See ISO 27036 for more information on supply chain security.