

INTERNATIONAL STANDARD

NORME INTERNATIONALE

AMENDMENT 1
AMENDEMENT 1

Security for industrial automation and control systems
Part 2-4: Security program requirements for IACS service providers
(standards.iteh.ai)

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

<https://standards.iteh.ai/catalog/standards/sist/1fd890c3-34a3-44f2-9fd2-57921833704a/iec-62443-2-4-2015-amd1-2017>





THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2017 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

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

Tel.: +41 22 919 02 11
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 corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform

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 It also gives information on projects, replaced and withdrawn publications.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 once a month by email.

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: sales@iec.ch.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22,000 terminological entries 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

67,000 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.

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.

Recherche de publications IEC -

webstore.iec.ch/advsearchform

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 une fois par mois par email.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

Electropedia - www.electropedia.org

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary

67 000 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.

INTERNATIONAL STANDARD

NORME INTERNATIONALE

AMENDMENT 1
AMENDEMENT 1

**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; 35.110

ISBN 978-2-8322-6486-7

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

FOREWORD

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

This bilingual version (20219-02) corresponds to the monolingual English version, published in 2017-08.

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.

The French version of this amendment has not been voted upon.

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.

(standards.iteh.ai)

[IEC 62443-2-4:2015/AMD1:2017](https://standards.iteh.ai/catalog/standards/sist/1fd890c3-34a3-44f2-9fd2-57921833704a/iec-62443-2-4-2015-amd1-2017)

<https://standards.iteh.ai/catalog/standards/sist/1fd890c3-34a3-44f2-9fd2-57921833704a/iec-62443-2-4-2015-amd1-2017>

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

iTeh STANDARD PREVIEW

5.5.7 Requirement description standards.iteh.ai

Add “column” to the title as follows:

[IEC 62443-2-4:2015/AMD1:2017](https://standards.iteh.ai/catalog/standards/sist/1fd890c3-34a3-44f2-9fd2-57921833704a/iec-62443-2-4-2015-amd1-2017)

<https://standards.iteh.ai/catalog/standards/sist/1fd890c3-34a3-44f2-9fd2-57921833704a/iec-62443-2-4-2015-amd1-2017>

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[IEC 62443-2-4:2015/AMD1:2017](https://standards.iteh.ai/catalog/standards/sist/1fd890c3-34a3-44f2-9fd2-57921833704a/iec-62443-2-4-2015-amd1-2017)
<https://standards.iteh.ai/catalog/standards/sist/1fd890c3-34a3-44f2-9fd2-57921833704a/iec-62443-2-4-2015-amd1-2017>

Annex A – Security requirements

Table A.1 – Security program requirements
Change the text in the “Requirement description” and “Rationale” columns to:
THE STANDARD PREVIEW
(standards.iec.ch)

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc	Requirement description	Rationale
SP.01.04	BR	Solution staffing	Background checks	Service provider	IEC 62443-2-4:2015/AMD1:2017 No. 3-347-1-10 57921833704a/iec-62443-2-4-2015-amd1-1-10	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	<p>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.</p>	<p>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.</p> <p>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.</p> <p>See ISO/IEC 27036-3 for additional supply chain organizational requirements.</p>

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		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.	<p>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.</p> <p>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.</p>

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	<p>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:</p> <ol style="list-style-type: none"> 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) <p>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.</p> <p>NOTE 2 Depending on the Automation Solution, Level 2/Level 3 interfaces may be "External" interface.</p>	<p>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).</p> <p>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.</p> <p>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.</p>

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 retention	?	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, turning 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.	<p>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.</p> <p>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.</p> <p>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.</p>