

# INTERNATIONAL STANDARD

## NORME INTERNATIONALE



**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**



## THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2015 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  
Fax: +41 22 919 03 00  
[info@iec.ch](mailto:info@iec.ch)  
[www.iec.ch](http://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](http://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](http://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](http://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](http://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](http://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](http://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](mailto: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](http://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](http://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](http://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](http://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](http://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](http://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](mailto:csc@iec.ch).

# INTERNATIONAL STANDARD

## NORME INTERNATIONALE



**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

**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.**

## CONTENTS

FOREWORD.....	3
INTRODUCTION.....	5
1 Scope.....	6
2 Normative references .....	7
3 Terms, definitions, abbreviated terms and acronyms .....	7
3.1 Terms and definitions .....	7
3.2 Abbreviations .....	10
4 Concepts.....	11
4.1 Use of IEC 62443-2-4.....	11
4.1.1 Use of IEC 62443-2-4 by IACS service providers .....	11
4.1.2 Use of IEC 62443-2-4 by IACS asset owners .....	12
4.1.3 Use of IEC 62443-2-4 during negotiations between IACS asset owners and IACS service providers .....	12
4.1.4 Profiles .....	12
4.1.5 IACS integration service providers.....	13
4.1.6 IACS maintenance service providers .....	13
4.2 Maturity model .....	14
5 Requirements overview.....	15
5.1 Contents .....	15
5.2 Sorting and filtering .....	15
5.3 IEC 62264-1 hierarchy model .....	16
5.4 Requirements table columns .....	16
5.5 Column definitions .....	16
5.5.1 Req ID column .....	16
5.5.2 BR/RE column .....	16
5.5.3 Functional area column .....	17
5.5.4 Topic column .....	18
5.5.5 Subtopic column .....	19
5.5.6 Documentation column.....	21
5.5.7 Requirement description.....	21
5.5.8 Rationale .....	21
Annex A (normative) Security requirements .....	22
Bibliography .....	85
Figure 1 – Parts of the IEC 62443 Series.....	5
Figure 2 – Scope of service provider capabilities .....	6
Table 1 – Maturity levels.....	15
Table 2 – Columns.....	16
Table 3 – Functional area column values.....	18
Table 4 – Topic column values .....	19
Table 5 – Subtopic column values .....	20
Table A.1 – Security program requirements.....	22

## INTERNATIONAL ELECTROTECHNICAL COMMISSION

**SECURITY FOR INDUSTRIAL AUTOMATION  
AND CONTROL SYSTEMS –****Part 2-4: Security program requirements  
for IACS service providers**

## FOREWORD

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

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

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

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

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

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

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

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

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

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

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

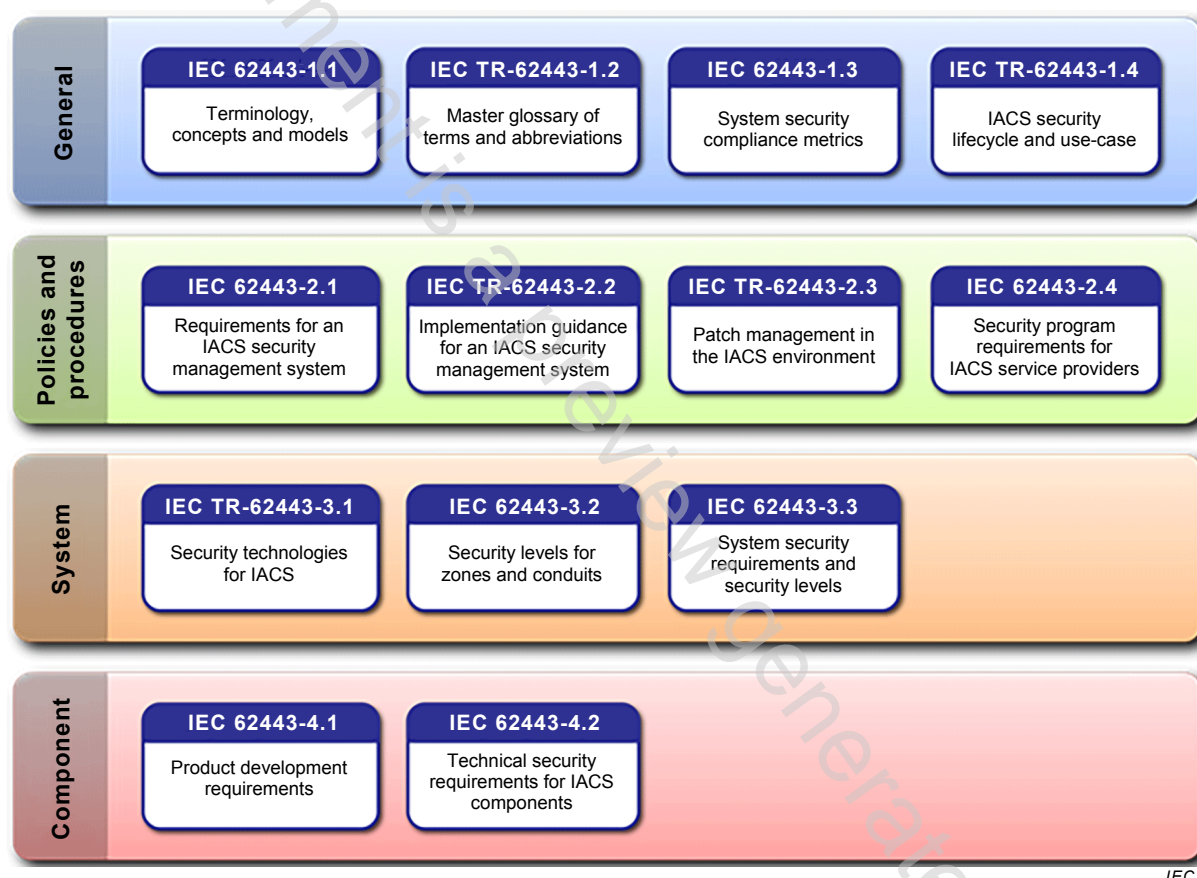
The contents of the corrigendum of August 2015 have been included in this copy.

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

## 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.



IEC

Figure 1 – Parts of the IEC 62443 Series

# SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

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

### 1 Scope

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

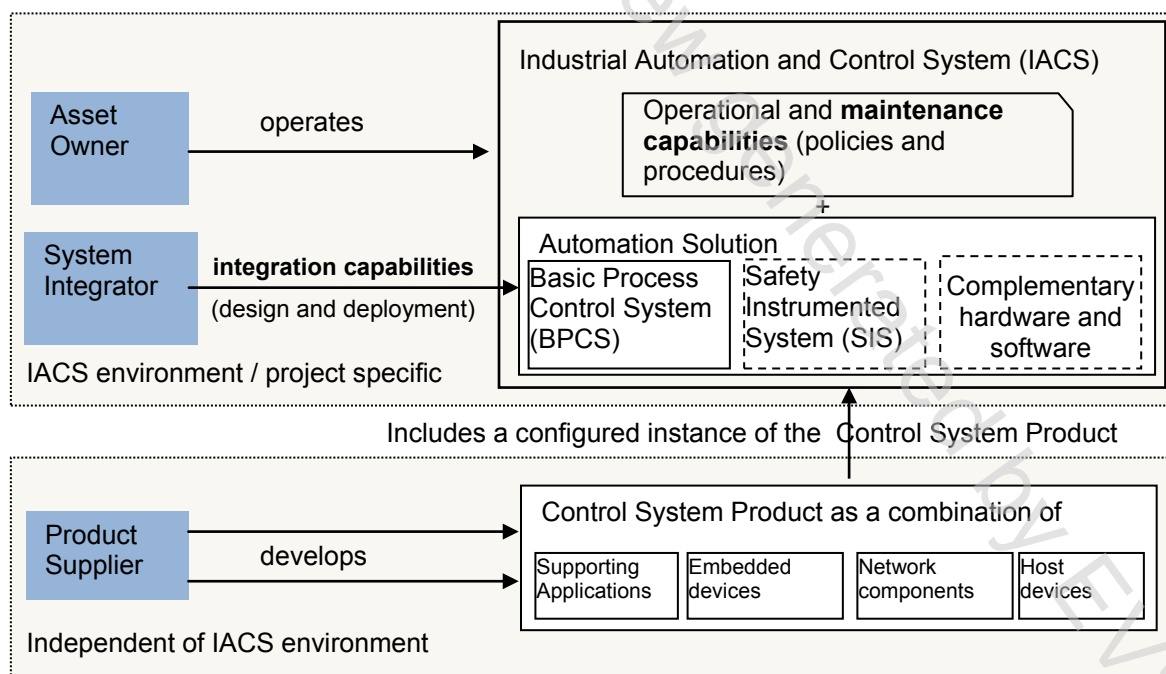


Figure 2 – Scope of service provider capabilities

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.