

PUBLICLY AVAILABLE SPECIFICATION

Security for industrial automation and control systems –
Part 2-2: IACS security protection scheme

(<https://standards.iteh.ai>)

Document Preview

[IEC PAS 62443-2-2:2025](https://standards.iteh.ai/catalog/standards/iec/46c84bf4-244e-471b-962c-19b16f1c4e99/iec-pas-62443-2-2-2025)

<https://standards.iteh.ai/catalog/standards/iec/46c84bf4-244e-471b-962c-19b16f1c4e99/iec-pas-62443-2-2-2025>



THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2025 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.

IEC Secretariat
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 It also gives information on projects, replaced and withdrawn publications.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.

IEC Products & Services Portal - products.iec.ch

Discover our powerful search engine and read freely all the publications previews, graphical symbols and the glossary. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 500 terminological entries in English and French, with equivalent terms in 25 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

International
Standards
Document Preview
standards.iteh.ai

[IEC PAS 62443-2-2:2025](http://standards.iteh.ai/catalog/standards/iec/46c84bf4-244e-471b-962c-19b16f1c4e99/iec-pas-62443-2-2-2025)

<https://standards.iteh.ai/catalog/standards/iec/46c84bf4-244e-471b-962c-19b16f1c4e99/iec-pas-62443-2-2-2025>



PUBLICLY AVAILABLE SPECIFICATION

**Security for industrial automation and control systems –
Part 2-2: IACS security protection scheme**

ITeH Standards
(<https://standards.iteh.ai>)
Document Preview

[IEC PAS 62443-2-2:2025](https://standards.iteh.ai/catalog/standards/iec/46c84bf4-244e-471b-962c-19b16f1c4e99/iec-pas-62443-2-2-2025)

<https://standards.iteh.ai/catalog/standards/iec/46c84bf4-244e-471b-962c-19b16f1c4e99/iec-pas-62443-2-2-2025>

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 25.040.40; 35.100.05

ISBN 978-2-8327-0299-4

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

CONTENTS

FOREWORD.....	4
INTRODUCTION.....	6
1 Scope.....	7
2 Normative references	7
3 Terms, definitions, abbreviated terms and acronyms	8
3.1 Terms and definitions.....	8
3.2 Abbreviated terms and acronyms	10
4 Relationship between this document and other documents	10
5 Security program and security protection scheme	11
5.1 Relationship between security program and security protection scheme.....	11
5.2 Process steps for the generation of a Security Protection Scheme	12
6 Security protection ratings	14
6.1 Overview.....	14
6.2 Use of the maturity model defined in IEC 62443-2-1 for the determination of SPR values	15
6.3 Use of alternative SPR matrixes for internal purposes.....	17
6.4 Grouping of security requirements	18
6.5 Tracing to SPEs and sub-SPEs.....	18
6.6 Views.....	19
6.7 SPR and SL types.....	20
6.7.1 General	20
6.7.2 SL types for products.....	20
6.7.3 SPR types used in an IACS life cycle.....	20
7 Principal roles.....	22
7.1 Overview.....	22
7.2 Asset owner	23
7.3 Integration service provider.....	24
7.4 Maintenance service provider	24
7.5 Product supplier.....	24
7.6 Other roles.....	25
8 Duties and activities in the IACS life cycle related to the security protection scheme.....	25
8.1 Overview.....	25
8.2 Generation of the cybersecurity requirement specification (CRS)	26
8.3 Design and implementation of the security measures	27
8.4 Generation and documentation of the process security measures	30
8.5 Validation of the security protection scheme	30
8.5.1 Overview	30
8.5.2 Validation of the technical security measures	31
8.5.3 Validation of the process security measures	32
8.5.4 Prediction of the SPR values, SPR-I	32
8.6 Periodic revalidation of the SPS during operation	33
Annex A (informative) Example of methodology for SPR verification	34
A.1 Overview.....	34
A.2 Detailed assessment, requirements-based	34
A.3 Detailed assessment, risk-based.....	35

A.4	Simplified evaluation, questions-based	35
Annex B (informative)	Maturity level assessment	36
B.1	General.....	36
B.2	Overall assessment work process	36
B.3	Maturity level assessment procedure	36
B.4	Security program maturity level assessment attributes	39
B.5	ML assessment documentation	42
Bibliography	44
Figure 1	– Simplified asset owner security protection scheme (SPS) life cycle	7
Figure 2	– Security program and security protection scheme	12
Figure 3	– Process steps for generating a security protection scheme	13
Figure 4	– Maturity model	15
Figure 5	– Determination of the SPR value by using the maturity model of IEC 62443-2-1	16
Figure 6	– Example of visualizing the fulfilment of a system security requirement with an SPR value.....	17
Figure 7	– Examples of alternative SPR matrix for internal purposes	18
Figure 8	– Example of a dashboard for the generic view	20
Figure 9	– Use of SPR and SL types in the IACS life cycle.....	22
Figure 10	– Roles and responsibilities overview	23
Figure 11	– Life cycle phases and roles	26
Figure 12	– Iterations in the IACS life cycle	26
Figure 13	– Activities and responsibilities for the generation of the CRS (simplified view).....	27
Figure 14	– Activities and responsibilities for the design and implementation of the technical security measures applied to the automation solution (simplified view).....	28
Figure 15	– Activities and responsibilities for the documentation of process security measures (simplified view).....	30
Figure 16	– Example of the determination of the SL value which can be met with capabilities provided by the technical security measures.....	31
Figure 17	– Example of the prediction of the SPR value.....	32
Figure B.1	– Example ML assessment based on IEC 62443-2-1.....	43
Table B.1	– Assessment MLs	36
Table B.2	– Maturity level assessment procedure	37
Table B.3	– Security program maturity level assessment attributes	39

INTERNATIONAL ELECTROTECHNICAL COMMISSION

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –**Part 2-2: IACS security protection scheme**

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) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at <https://patents.iec.ch>. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 62443-2-2 has been prepared by IEC technical committee 65: Industrial-process measurement, control and automation. It is a Publicly Available Specification.

IEC PAS 62443-2-2 has been developed by IEC TC 65 and the liaison ISA99: ISA committee on Security for industrial automation and control systems.

The text of this Publicly Available Specification is based on the following documents:

Draft	Report on voting
65/1051/DPAS	65/1121/RVDPAS

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

The language used for the development of this Publicly Available Specification is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, and the ISO/IEC Directives, JTC 1 Supplement available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

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.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

NOTE In accordance with ISO/IEC Directives, Part 1, IEC PASs are automatically withdrawn after 4 years.

iTeh Standards (<https://standards.iteh.ai>) Document Preview

[IEC PAS 62443-2-2:2025](https://standards.iteh.ai/catalog/standards/iec/46c84bf4-244e-471b-962c-19b16f1c4e99/iec-pas-62443-2-2-2025)

<https://standards.iteh.ai/catalog/standards/iec/46c84bf4-244e-471b-962c-19b16f1c4e99/iec-pas-62443-2-2-2025>

INTRODUCTION

This document is the part of the IEC 62443 series that provides guidance on the development and validation of a set of technical, physical, and process security measures to address risk associated with cyberthreats when operating IACS. In the context of this document, asset owner also includes the operator of the IACS.

The purpose of the document is to provide input to support asset owners, integration service providers, maintenance service providers as well as product suppliers in their activities to provide a combination of technical, physical, and organizational capabilities for protecting IACS against cyberthreat.

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[IEC PAS 62443-2-2:2025](https://standards.iteh.ai/catalog/standards/iec/46c84bf4-244e-471b-962c-19b16f1c4e99/iec-pas-62443-2-2-2025)

<https://standards.iteh.ai/catalog/standards/iec/46c84bf4-244e-471b-962c-19b16f1c4e99/iec-pas-62443-2-2-2025>

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 2-2: IACS security protection scheme

1 Scope

This part of IEC 62443 provides guidance on the development, validation, operation, and maintenance of a set of technical, physical, and process security measures called Security Protection Scheme (SPS). The document's goal is to provide the asset owner implementing an IACS Security Program (SP) with mechanisms and procedures to ensure that the design, implementation and operation of an SPS manage the risks resulting from cyberthreats to each of the IACS included in its operating facility.

The document is based on contents specified in other documents of the IEC 62443 series and explains how these contents can be used to support the development of technical, physical, and process security measures addressing the risks to the IACS during the operation phase.

Figure 1 illustrates the content of this document using a simplified IACS life cycle.

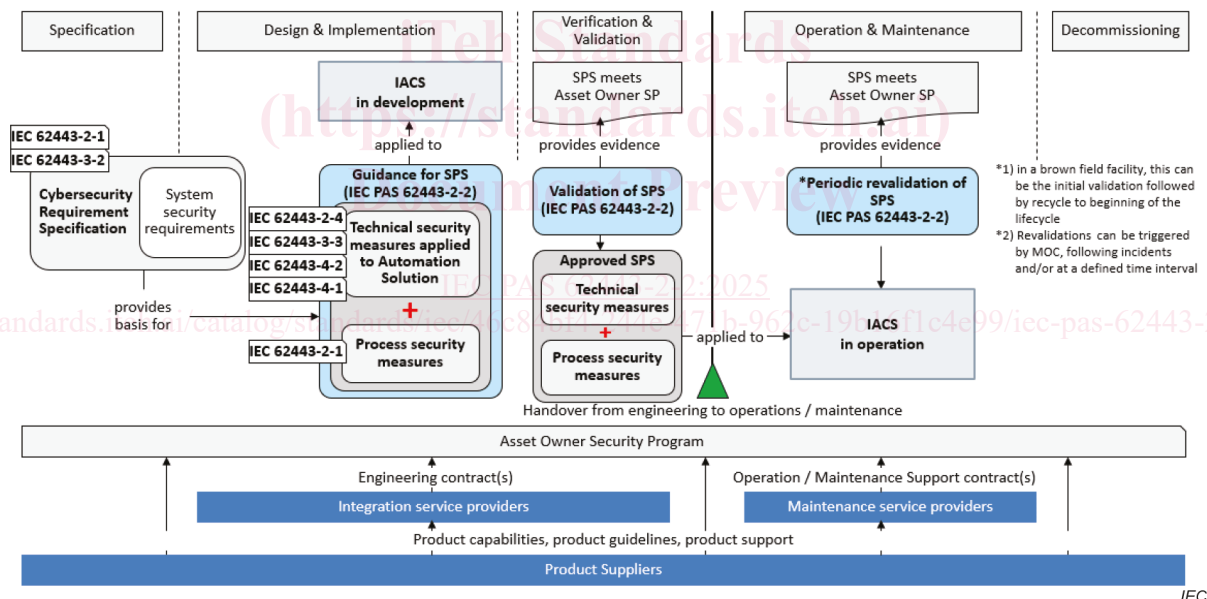


Figure 1 – Simplified asset owner security protection scheme (SPS) life cycle

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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.

IEC TS 62443-1-1:2009, *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*

IEC 62443-2-1:—¹, *Security for industrial automation and control systems – Part 2-1: Security program requirements for IACS asset owners*

IEC 62443-2-4:2023, *Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers*

IEC 62443-3-2:2020, *Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design*

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

3 Terms, definitions, abbreviated terms and acronyms

For the purposes of this document, the terms and definitions given in IEC TS 62443-1-1 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <https://www.electropedia.org/>
- ISO Online browsing platform: available at <https://www.iso.org/obp>

NOTE Terms and definitions are defined in IEC TS 62443-1-1. The purpose of this clause is to provide supplemental guidance for some key terms used in this document, to improve clarity for the reader.

3.1 Terms and definitions

3.1.1

security program

SP

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 SP for IACS asset owners refers to the policies and procedures defined by them to address cybersecurity concerns of the IACS. This can include technical, process, physical and compensating security measures used to reduce the cybersecurity attack surface.

[SOURCE: IEC 62443-2-1:—, 3.1.15]

3.1.2

security protection scheme

SPS

set of technical, physical, and process security measures designed to address cyber security concerns of an IACS during operation

Note 1 to entry: The SP for IACS asset owners refers to the policies and procedures defined by them to address cybersecurity concerns of the IACS. This can include technical, process, physical and compensating security measures used to reduce the cybersecurity attack surface.

¹ Under preparation. Stage at the time of publication: IEC/FDIS 62443-2-1:2024.

3.1.3

system security requirement

security requirements based on requirements specified in IEC 62443-3-3:2013

Note 1 to entry: When applied to products, the system security requirements are specified in IEC 62443-3-3:2013. Each requirement is formulated as "The control system shall provide the capability to ...".

Note 2 to entry: When applied to automation solutions, the system security requirements are defined as "The zone of the automation solution shall provide the capability to ...", instead of "The control system shall provide the capability to ...".

Note 3 to entry: When applied to IACS in operation, the system security requirements are defined as "The IACS in operation shall provide the capability to ...", instead of "The control system shall provide the capability to ...".

3.1.4

security level

measure of confidence that the IACS is free from vulnerabilities and functions in the intended manner

Note 1 to entry: The definition of security levels is expected to evolve. In the context of this document, the security levels are the levels to which the system security requirements are mapped to according to IEC 62443-3-3.

[SOURCE: IEC 62443-3-3:2013: 3.1.38, modified – The Note to entry has been changed.]

3.1.5

target security protection ratings

levels of the system security requirements that an asset owner desires to be fulfilled during operation

3.1.6

implemented security protection ratings

levels of the system security requirements which can be fulfilled during implementation by the designed technical, physical, and process security measures, under the assumption that the process security measures will be executed during operation with a demonstrated repeatability and effectiveness

3.1.7

operated security protection ratings

levels of system security requirements that have been fulfilled by the technical, physical, and process security measures at a given point of time during operation, with demonstrated process security measures that are repeatable and effective

3.1.8

maturity level

qualitative method of characterizing the capability of an organization to implement security requirements according to documented policies and procedures and their historical performance in doing so

Note 1 to entry: In the context of this document, maturity levels express the level of confidence that process security measures are executed by the personnel in charge during operation of the IACS with a demonstrated repeatability and effectiveness.

[SOURCE: IEC 62443-2-1:—, 3.1.7, modified – The Note to entry has been added.]

3.1.9

security measure

measure taken for an IACS to protect the safety, integrity, availability, and confidentiality

[SOURCE: IEC TS 62443-1-1:—, 3.1.110]

3.2 Abbreviated terms and acronyms

AO	asset owner
CRS	cybersecurity requirements specification
IACS	industrial automation and control systems
IEC	International Electrotechnical Commission
ISA	International Society of Automation
ISO	International Organization for Standardization
KPI	key performance indicator
ML	maturity level
MS	maintenance service provider
NIST	National Institute of Standards and Technology
PS	product supplier
SI	integration service provider
SL	security level
SL-C	security level capability
SP	security program
SPE	security program element
SPR	security protection rating
SPR-I	security protection rating implemented
SPR-O	security protection rating operational
SPR-T	security protection rating target
SPS	security protection scheme
SR	security requirement
SuC	system under consideration

4 Relationship between this document and other documents

The document describes the activities for the design, implementation, and validation of an SPS and the use of IEC 62443-2-1, IEC 62443-2-4, IEC 62443-3-2, IEC 62443-3-3, IEC 62443-4-1, and IEC 62443-4-2 for supporting these activities.

The concepts described in this document are not all reflected in currently published documents of the IEC 62443 series. None of these concepts contradicts contents of the IEC 62443 documents. They provide input for evolutions, which are expected to be reflected in further editions of IEC 62443 series documents.