



International Society of Automation
Setting the Standard for Automation™

**TECHNICAL
REPORT**

ISA-TR62443-2-2-2025

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

Approved: 26 MAY 2025

© 2025 International Society of Automation. This is a copyright document and may not be copied or distributed in any form or manner without the permission of ISA. This copy of the document was made for the sole use of the person to whom ISA provided it and is subject to the restrictions stated in the *Copyright of ISA Standards* policy. It may not be provided to any other person in print, electronic or any other form. Violations of ISA's copyright will be persecuted to the fullest extent of the law and may result in substantial civil and criminal penalties.

Documents
Document Sharing Hub

ISA-TR62443-2-2-2025

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

ISBN: 978-1-64331-276-7

Copyright © 2025 by the International Society of Automation (ISA). All rights reserved. Not for resale. Printed in the United States of America. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the prior written permission of the Publisher.

ISA
3252 S. Miami Blvd., Suite 102
Durham, NC 27703 USA

PREFACE

This preface is included for information and is not a normative part of ISA-TR62443-2-2-2025.

This document has been prepared as part of the service of ISA toward a goal of uniformity in the field of automation. To be of real value, this document should not be static but should be subject to periodic review. Toward this end, the Society welcomes all comments and criticisms and asks that they be addressed to the Secretary, ISA Standards and Practices Board; standards@isa.org.

It is the policy of ISA to encourage and welcome the participation of all concerned individuals and interests in the development of ISA standards, recommended practices, and technical reports. Participation in the ISA standards-making process by an individual in no way constitutes endorsement by the employer of that individual, of ISA, or of any of the standards, recommended practices, and technical reports that ISA develops.

International System of Units (SI) are the preferred units of measurement in ISA standards.

CAUTION — ISA ADHERES TO THE POLICY OF THE AMERICAN NATIONAL STANDARDS INSTITUTE WITH REGARD TO PATENTS. IF ISA IS INFORMED OF AN EXISTING PATENT THAT IS REQUIRED FOR USE OF THE DOCUMENT, IT WILL REQUIRE THE OWNER OF THE PATENT TO EITHER GRANT A ROYALTY-FREE LICENSE FOR USE OF THE PATENT BY USERS COMPLYING WITH THE DOCUMENT OR A LICENSE ON REASONABLE TERMS AND CONDITIONS THAT ARE FREE FROM UNFAIR DISCRIMINATION.

EVEN IF ISA IS UNAWARE OF ANY PATENT COVERING THIS DOCUMENT, THE USER IS CAUTIONED THAT IMPLEMENTATION OF THE DOCUMENT MAY REQUIRE USE OF TECHNIQUES, PROCESSES, OR MATERIALS COVERED BY PATENT RIGHTS. ISA TAKES NO POSITION ON THE EXISTENCE OR VALIDITY OF ANY PATENT RIGHTS THAT MAY BE INVOLVED IN IMPLEMENTING THE DOCUMENT. ISA IS NOT RESPONSIBLE FOR IDENTIFYING ALL PATENTS THAT MAY REQUIRE A LICENSE BEFORE IMPLEMENTATION OF THE DOCUMENT OR FOR INVESTIGATING THE VALIDITY OR SCOPE OF ANY PATENTS BROUGHT TO ITS ATTENTION. THE USER SHOULD CAREFULLY INVESTIGATE RELEVANT PATENTS BEFORE USING THE DOCUMENT FOR THE USER'S INTENDED APPLICATION.

HOWEVER, ISA ASKS THAT ANYONE REVIEWING THIS DOCUMENT WHO IS AWARE OF ANY PATENTS THAT MAY IMPACT IMPLEMENTATION OF THE DOCUMENT NOTIFY THE ISA STANDARDS AND PRACTICES DEPARTMENT OF THE PATENT AND ITS OWNER.

ADDITIONALLY, THE USE OF THIS DOCUMENT MAY INVOLVE HAZARDOUS MATERIALS, OPERATIONS OR EQUIPMENT. THE DOCUMENT CANNOT ANTICIPATE ALL POSSIBLE APPLICATIONS OR ADDRESS ALL POSSIBLE SAFETY ISSUES ASSOCIATED WITH USE IN HAZARDOUS CONDITIONS. THE USER OF THIS DOCUMENT MUST EXERCISE SOUND PROFESSIONAL JUDGMENT CONCERNING ITS USE AND APPLICABILITY UNDER THE USER'S PARTICULAR CIRCUMSTANCES. THE USER MUST ALSO CONSIDER THE APPLICABILITY OF ANY GOVERNMENTAL REGULATORY LIMITATIONS AND ESTABLISHED SAFETY AND HEALTH PRACTICES BEFORE IMPLEMENTING THIS DOCUMENT.

THE USER OF THIS DOCUMENT SHOULD BE AWARE THAT THIS DOCUMENT MAY BE IMPACTED BY ELECTRONIC SECURITY ISSUES. THE COMMITTEE HAS NOT YET ADDRESSED THE POTENTIAL ISSUES IN THIS VERSION.

ISA (www.isa.org) is an international professional association that sets the standard for those who apply engineering and technology to improve the management, safety, and cybersecurity of modern automation and control systems used across industry and critical infrastructure. Founded in 1945, ISA develops widely used international standards for industrial automation, safety, and cybersecurity; certifies industry professionals; provides education and training; publishes books

and technical articles; hosts conferences and events; and provides networking and career development programs for its members and customers around the world.

ISA owns Automation.com, a leading online publisher of automation-related content. In addition, through a wholly owned subsidiary, ISA bridges the gap between standards and their implementation with the ISA Security Compliance Institute (www.isasecure.org) and the ISA Wireless Compliance Institute (www.isa100wci.org).

The following people served as active members of ISA99 Working Group 03, Task Group 03 for the preparation of this document:

Name	Company	Contributor	Reviewer
Pierre Kobes, TG chair	Dr. Kobes Consulting	X	
Swarandeeep Singh, TG editor	ABB	X	
Khalid Ansari	FM Approvals	X	
Jens Braband	Siemens AG		X
Marcelo Branquinho	Tisafe Segurana Da Informau Ltd		X
Steve Cauduro	McCain Foods		X
Vincent Chiew	Axis Cogni-Solve Ltd	X	
Eric Cosman	OIT Concepts, LLC	X	
Bill Cotter	Consultant		X
Ed Crawford	Consultant		X
Gonzalo Curiel Fernandez	ProcesSkills		X
Todd Brent Davis	Vestas	X	
Sami El-Murr	Hunter Strategy LLC	X	
Gabriel Faifman	Schneider Electric	X	
Pedro Fernandes	Consultant	X	
Jim Gilsinn	MITRE	X	
Jean-Pierre Hauet	KB Intelligence	X	
Eric Hopp	Symbotic		X
Greg Hudson	Metcalfe PLLC		X
Peter Jackson	SGS		X
Mats Karlsson	Sectra		X
Erwin Kruschitz	Anapur	X	
Karen Kuhn	Cenovus Energy	X	
Suzanne Lightman	NIST	X	
Claudia Lutze	Thales	X	
Ken Masica	Lawrence Livermore National Lab	X	
Mike Medoff	Exida		X
Glenn Merrell	Industrial Control Systems Security	X	
Roberto Minicucci	GE Vernova	X	
Alex Nicoll	Rockwell Automation	X	
Lee Neitzel	Consultant	X	
Johan Nye	ICS Guru LLC	X	
Vijay Pushpanathan	General Electric Research	X	
Sharul A Rashid	TI Consultancy		X
Gary Rathwell	Entercon	X	

Name	Company	Contributor	Reviewer
Francisco Rivero	Iberdrola		X
Judith Rossebo	ABB AS	X	
Maik Seewald	Cisco	X	
Kevin Staggs	Consultant	X	
Michael Theuerzeit	Hudson Cybertec	X	
Ilya Tillekens	Hudson Cybertec	X	
Brad Taylor	Consultant		X
Hal Thomas	HWT Consulting, LLC	X	
Bill Thomson	Exida		X
Ted Trost	Cargill		X
Paulo Vergara	Zavior Consulting		X
Christine van Vredendaal	NXP Semiconductors	X	
Jens Wiesner	BSI	X	
Markus Wischy	Siemens Rail Automation	X	
Ben White	OPSWAT		X
Kai Wollenweber	Siemens AG	X	
Fan Ye	WSP	X	
Mohamed Youssef	SecuriCIP		X
Bob Zapata	Zapata Technical Group LLC	X	
Andrew Zwart	Northridge Cybersecurity	X	

This document was approved by the ISA Standards and Practices Board on 26 May 2025:

NAME

AFFILIATION

D. Brandl, *Chair*
D. Board, *Chair-Elect*
D. Bartusiak
P. Brett
E. Cosman
J. Federlein
S. Fluchs
J.-P. Hauet
D. Lee
G. Lehmann
T. McAvinew
V. Mezzano
C. Monchinski
I. Verhappen
D. Visnich
J. Weiss
D. Zetterberg

BR&L Consulting
Yokogawa
Collaborative Systems Integration
Honeywell
OIT Concepts
Federlein & Associates
admeritia GmbH
KB Intelligence
UCDS
NextEra Energy
Consultant
Fluor Corp
Automated Control Concepts
Willowglen Systems
Burns & McDonnell
Applied Control Solutions
Consultant

This page intentionally left blank.

CONTENTS

FOREWORD	9
INTRODUCTION	11
1 Scope	13
2 Normative references	13
3 Terms, definitions, abbreviated terms and acronyms	14
3.1 Terms and definitions.....	14
3.2 Abbreviated terms and acronyms	15
4 Relationship between this document and other documents	16
5 Security program and security protection scheme	16
5.1 Relationship between security program and security protection scheme	16
5.2 Process steps for the generation of a Security Protection Scheme	17
6 Security protection ratings	19
6.1 Overview	19
6.2 Use of the maturity model defined in ISA-62443-2-1 for the determination of SPR values.....	19
6.3 Use of alternative SPR matrices for internal purposes.....	22
6.4 Grouping of security requirements.....	23
6.5 Tracing to SPEs and sub-SPEs	23
6.6 Views	24
6.7 SPR and SL types.....	25
6.7.1 General	25
6.7.2 SL types for products.....	25
6.7.3 SPR types used in an IACS life cycle	25
7 Principal roles	27
7.1 Overview	27
7.2 Asset Owner.....	27
7.3 Integration Service Provider	28
7.4 Maintenance Service Provider.....	28
7.5 Product Supplier	28
7.6 Other roles	29
8 Duties and activities in the IACS life cycle related to the Security Protection Scheme ...	29
8.1 Overview	29
8.2 Generation of the Cybersecurity Requirement Specification (CRS)	31
8.3 Design and implementation of the security measures	31
8.4 Generation and documentation of the process security measures	34
8.5 Validation of the Security Protection Scheme.....	34
8.5.1 Overview	34
8.5.2 Validation of the technical security measures	34
8.5.3 Validation of the process security measures	35
8.5.4 Prediction of the SPR values, SPR-I.....	36

8.6	Periodic revalidation of the SPS during operation	36
Annex A (informative)	Example of methodology for SPR verification	39
A.1	Overview	39
A.2	Detailed assessment, requirements-based	39
A.3	Detailed assessment, risk-based	40
A.4	Simplified evaluation, questions-based	40
Annex B (informative)	Maturity level assessment	41
B.1	Introduction	41
B.2	Overall assessment work process	41
B.3	Maturity level assessment procedure	42
B.4	Security program maturity level assessment attributes	43
B.5	ML assessment documentation	47
BIBLIOGRAPHY		49
Figure 1	– Simplified asset owner Security Protection Scheme (SPS) life cycle	13
Figure 2	– Security Program and Security Protection Scheme	17
Figure 3	– Process steps for generating a Security Protection Scheme	18
Figure 4	– Maturity model	20
Figure 5	– Determination of the SPR value by using the maturity model of ISA-62443-2-1	21
Figure 6	– Example of visualizing the fulfillment of a system security requirement with an SPR value	22
Figure 7	– Examples of alternative SPR matrix for internal purposes	23
Figure 8	– Example of a dashboard for the generic view	25
Figure 9	– Use of SPR and SL types in the IACS life cycle	26
Figure 10	– Roles and responsibilities overview	27
Figure 11	– Life cycle phases and roles	30
Figure 12	– Iterations in the IACS life cycle	30
Figure 13	– Activities and responsibilities for the generation of the CRS (simplified view)	31
Figure 14	– Activities and responsibilities for the design and implementation of the technical security measures applied to the Automation Solution (simplified view)	32
Figure 15	– Activities and responsibilities for the documentation of process security measures (simplified view)	34
Figure 16	– Example of the determination of the SL value which can be met with capabilities provided by the technical security measures	35
Figure 17	– Example of the prediction of the SPR value	36
Figure B.1	– Example ML assessment based on ISA-62443-2-1	48
Table B.1	– Assessment MLs	41
Table B.2	– Maturity level assessment procedure	42
Table B.3	– Security program maturity level assessment attributes	43

FOREWORD

This document is part of a multipart standard that addresses the issue of security for industrial automation and control systems. It has been developed by ISA99 Working Group 03, Task Group 03 in collaboration with IEC TC65 / WG10

This document prescribes the requirements to perform a rating of the expected level of protection provided by technical and process security measures during the operation of an IACS.

This page intentionally left blank.

INTRODUCTION

This document is the part of the ISA-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, and 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.

This page intentionally left blank.

1 Scope

This document 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 ISA-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.

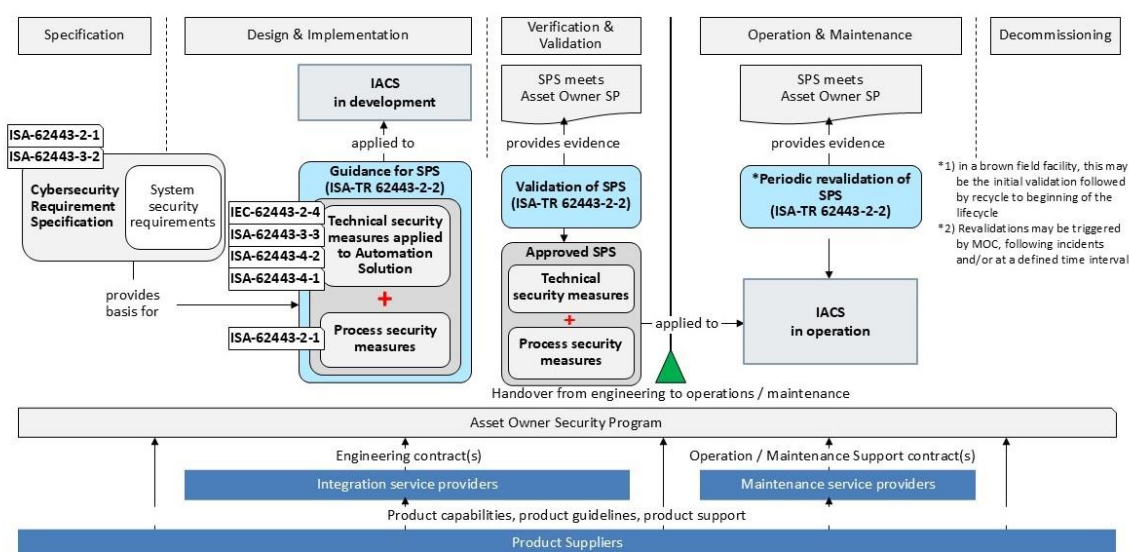


Figure 1 – Simplified asset owner Security Protection Scheme (SPS) life cycle

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.

ISA-62443-1-1-2007, *Security for industrial automation and control systems – Part 1-1: Terminology, concepts and models*

ISA-62443-2-1-2024, *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*

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

ISA-62443-3-3-2013, *Security for industrial automation and control systems – 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 ISA-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 ISA-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: ISA-62443-2-1-2024, 3.1.15, modified – removed the source Note 1 to entry]

3.1.2

security protection scheme

SPS

set of technical, physical, and process security measures designed to address cybersecurity 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.

3.1.3

system security requirement

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

Note 1 to entry: When applied to products, the system security requirements are specified in ISA-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

[SOURCE: ISA-62443-3-3:2013]

NOTE 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 ISA-62443-3-3.

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: ISA-62443-2-1-2024, 3.1.7]

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 ISA-62443-2-1, IEC 62443-2-4, ISA-62443-3-2, ISA-62443-3-3, ISA-62443-4-1, and ISA-62443-4-2 for supporting these activities.

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

5 Security program and security protection scheme

5.1 Relationship between security program and security protection scheme

ISA-62443-2-1 specifies security program (SP) requirements for IACS asset owners. The SP of IACS asset owners refers to technical, physical, and process security measures defined by them to address cybersecurity concerns of all the IACS during their respective life cycle. The SP can include technical, physical, and process security measures to reduce the cybersecurity attack surface. The SP also includes physical measures to reduce access to the assets of the IACS.

ISA-62443-2-1 has a requirement for the SP to implement an information security management system ensuring the execution of actions to reduce the risks. For an asset owner, risk reduction means the implementation of the necessary security measures for the protection of its operating facility against cyberthreats. It is not unusual that an operating facility includes several IACS, each of them controlling a part of the physical process. According to the criticality for the business of the asset owner, each IACS can have different target levels for security protection. The risk reduction actions include for each IACS the development of a set of technical, physical, and process security measures—the security protection scheme (SPS)—to meet the required target security protection levels. An asset owner establishing a Security Program ensures that an SPS is designed and applied during operation for each IACS, involving all roles defined in the ISA-62443 series.

The SPS life cycle is identical to the life cycle of the IACS to which the SPS is applied. In addition to security measures applied to each IACS, the SP includes security measures to meet corporate organization requirements of the operating facility. These are linked to the enterprise life cycle of the operating facility which is decoupled from the IACS / SPS life cycles. Examples of those measures are security management policies and procedures, security measurements such as KPIs, escalation procedures, top management reports, etc.