



International Society of Automation
Setting the Standard for Automation™

STANDARD

American National Standard ANSI/ISA-62443-2-1-2024

This standard is intended for worldwide use in all industries as applicable.

Security for industrial automation and control systems, Part 2-1: Security program requirements for IACS asset owners

Approved: 24 October 2024

© 2024 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

ANSI/ISA-62443-2-1-2024, Security industrial automation and control systems, Part 2-1: Security program requirements for IACS asset owners

ISBN: 978-1-64331-264-4

Copyright © 2024 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, as well as all footnotes and annexes, is included for information purposes and is not part of ANSI/ISA-62443-2-1-2024.

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 2 for the preparation of this document:

Name	Company	Contributor	Reviewer
Jim Gilsinn, WG Co-Chair	MITRE	X	
Meredith Allen	Metcalfe, PLLC	X	
Soloman Almadi	Aramco		X
Ken Anderson	ACKS Advisory Inc.	X	
Subodh Belgil	Individual	X	
Rudy Belliardi	Individual	X	
Rahul Bhojani	BP	X	
Sergei Biberdorf	TÜV Rheinland AG	X	
Thomas Bleier	B-SEC Better Secure KG	X	
Bill Bosler	Texas Consultants Inc.	X	
Dennis Brandl	BRL Consulting	X	
Tanya Brewer	NIST	X	
Riemer Brouwer	Booz, Allen, Hamilton	X	
Eric Byres	Byres Security		X
Matteo Camprini	Individual	X	
Antony Capel	Comgate		X
Jacob Chapman	Nozomi Networks	X	
Piotr Ciepiela	Ernst & Young	X	
Richard Clark	Wonderware		X
Eric Cosman, ISA99 Co-Chair	OIT Concepts LLC	X	
John Cusimano	Armexa, LLC	X	
Todd Brent Davis	Vestas	X	
Suzanne de Grooth – Verlijdsdonk	Actemium	X	
Jan de Meer	smartspacelab.eu GmbH	X	
Ronald Derynck	Verano		X
Gabriel Dimowo	Shell	X	
Robert Evans	Individual	X	
Gabriel Faifman	Schneider Electric	X	

Patrick Feeley	Rockwell Automation	X	
Junya Fujita	Hitachi Ltd.	X	
Didier Giarratano	Schneider Electric	X	
Camilo Gomez	Yokogawa	X	
Facundo Gomila	Tenaris	X	
Daniel Gonzalez	Schneider Electric	X	
Tom Good	Individual	X	
Donna Guillen	INL		X
Evan Hand	Individual	X	
Jean-Pierre Hauet	Inforoutes Ardeche		X
Ernie Hayden	Jacobs Engineering	X	
Mark Heard	TMD Consulting		X
Marnix Haije	Shell	X	
Greg Hudson	Metcalf, PLLC	X	
Markus Jans	Capgemini	X	
Nicholas S. Jones	Ersnt & Young	X	
Hiroo Kanamaru	Mitsubishi Electric Corp	X	
Sharad Karve	Individual		X
Pierre Kobes	Kobes Consulting	X	
Christian Kollmetzer	Individual	X	
Michael Krause	TUV Rheinland i-sec GmbH	X	
Joel Langill	ICS Cyber Security Institute LLC		X
Lakshmi Saroja Ponakala	Cummins	X	
Juan José López González	Cognizant	X	
Glenn Merrell	Freelance Consulting	X	
Dave Mills	Proctor and Gamble	X	
Carol Muehrcke	Cyber Defense Agency LLC	X	
Mike Nash	Gamma Secure Systems Ltd	X	
Lee Neitzel	Emerson Process Management	X	
Alex Nicoll	Rockwell Automation	X	
Johan Nye	ICS Guru LLC	X	
Patrick O'Brien	Exida LLC	X	
Richard Ikenobe Osolease	RGB Professional Services, LLC.	X	
Richard Oyen	Oyen Industrial Inc.	X	
Daniel Paillet	Schneider Electric	X	
Tom Phinney	Individual		X
Jeff Potter	Emerson		X
Hector Puyosa Pina	SABIC	X	
George Robertson	Chevron	X	
Matt Rollinson	Monsanto	X	
Judith Rossebo	ABB	X	

Ichikawa Sachika	Individual	X	
Denrich Sananda	Arista Technologies Ltd.	X	
Nicholas Sands	DuPont	X	
Rainer Schrundner	Sew-Eurodrive	X	
Peter Seiber	Cal Poly Pomona	X	
Bryan Singer	Accenture	X	
Martin Solum	Cyber Defense Agency LLC	X	
Charlie Souza	AcuTech Consulting Group	X	
Graham Speake	Accenture	X	
Leon Steinocher	Redstone Investors		X
Ivan Susanto	Chevron		X
Brad Taylor	Virtual Common Ground		X
Ian Verhappen	Willowglen Systems Inc.	X	
Jacek Walaszczyk	Ernst & Young	X	
Bob Webb	ICS Secure LLC		X
Ingo Weber	Siemens AG DI FA	X	
Joe Weiss	Applied Control Solutions, LLC	X	
Ludwig Winkel	Siemens	X	
Kai Wollenweber	Siemens	X	
Jeanne Wood	Matrikon	X	
Fan Ye	Engineering Safety Consultants	X	
Yoshimatso Kenzo	Individual	X	
Saber Zrelli	Yokogawa	X	

This standard was approved for publication by the ISA Standards and Practices Board on 30 September 2024:

NAME**AFFILIATION**

P. Brett	Honeywell
D. Bartusiak	Collaborative Systems Integration, Inc.
D. Board	Yokogawa
D. Brandl	BR&L Consulting, Inc.
E. Cosman	OIT Concepts LLC
J. Federlein	Federlein & Assoc LLC
S. Fluchs	Admeritia GmbH
J-P. Hauet	Hauet.Com
D. Lee	UCDS Inc.
G. Lehmann	NextEra Energy Resources
T. McAviney	Consultant
V. Mezzano	Fluor Corp.
C. Monchinski	Automated Control Concepts Inc.
I. Verhappen	Willowglen Systems Inc.
D. Visnich	Burns & McDonnell
J. Weiss	Applied Control Solutions LLC
D. Zetterberg	Consultant

IN MEMORIAM

Meredith Margaret Allen

In August 2018, ISA99 Working Group 2 lost one of its most active members with the passing of Meredith Allen. Meredith first joined the working group in 2010 as it was beginning its effort to develop the second edition of the ISA-62443-2-1 standard, becoming recognized as a voting member during her time on the ISA99 committee. She was instrumental in driving the working group toward the completion of the second edition. Meredith was a registered professional engineer in controls engineering and a project management professional. She was very passionate about the proper treatment of functional safety and cyber security within her profession. Her dedication to the committee and working group are reflected in this standard.

This page intentionally left blank.

CONTENTS

IN MEMORIAM	7
FOREWORD	15
INTRODUCTION	17
1 Scope	19
2 Normative references	20
3 Terms, definitions, abbreviated terms, acronyms and conventions	20
3.1 Terms and definitions.....	20
3.2 Abbreviated terms and acronyms	24
3.3 Conventions	26
4 Concepts	26
4.1 Use of this document	26
4.1.1 Applicable roles	26
4.1.2 Use of this document by asset owners	27
4.1.3 Use of this document by service providers and product suppliers	29
4.2 Maturity level (ML) definitions	30
4.3 Security levels (SLs)	31
4.4 Requirements definitions.....	32
4.4.1 Requirements organization	32
4.4.2 Requirements cross-references.....	32
4.4.3 Requirement conventions.....	32
5 Conformance and assessment.....	33
5.1 Overview	33
5.2 Conformity evidence	34
5.3 Requirements evaluation and profiles	34
5.3.1 Overview	34
5.3.2 Evaluation of risk to requirements	35
5.3.3 Profiles.....	35
5.3.4 Conformity assessment for the Asset Owner role.....	35
6 SPE 1 – Organizational security measures.....	36
6.1 Purpose.....	36
6.2 ORG 1 – Security related organization and policies	36
6.2.1 ORG 1.1: Information security management system (ISMS)	36
6.2.2 ORG 1.2: Background checks	36
6.2.3 ORG 1.3: Security roles and responsibilities	37
6.2.4 ORG 1.4: Security awareness training	37
6.2.5 ORG 1.5: Security responsibilities training.....	38
6.2.6 ORG 1.6: Supply chain security	39
6.3 ORG 2 – Security assessments and reviews.....	39
6.3.1 ORG 2.1: Security risk mitigation	39
6.3.2 ORG 2.2: Processes for discovery of security anomalies	40

6.3.3	ORG 2.3: Secure development and support	41
6.3.4	ORG 2.4: SP reviews	41
6.4	ORG 3 – Security of physical access	42
6.4.1	ORG 3.1: Physical access control	42
7	SPE 2 – Configuration management	42
7.1	Purpose.....	42
7.2	CM 1 – Inventory management of IACS hardware/software components and network communications	42
7.2.1	CM 1.1: Asset inventory baseline	42
7.2.2	CM 1.2: Infrastructure drawings/documentation	43
7.2.3	CM 1.3: Configuration settings	44
7.2.4	CM 1.4: Change control	44
8	SPE 3 – Network and communications security	45
8.1	Purpose.....	45
8.2	NET 1 – System segmentation	45
8.2.1	NET 1.1: Segmentation from non-IACS zones	45
8.2.2	NET 1.2: Documentation of zones and network zone interconnections	45
8.2.3	NET 1.3: Network segmentation from safety systems.....	46
8.2.4	NET 1.4: Network autonomy	46
8.2.5	NET 1.5: Network disconnection from external networks	47
8.2.6	NET 1.6: Internal network access control	47
8.2.7	NET 1.7: Network accessible services.....	47
8.2.8	NET 1.8: User messaging	48
8.2.9	NET 1.9: Network time distribution	48
8.3	NET 2 – Secure wireless access	49
8.3.1	NET 2.1: Wireless protocols.....	49
8.3.2	NET 2.2: Wireless network segmentation	49
8.3.3	NET 2.3: Wireless properties and addresses	50
8.4	NET 3 – Secure remote access	50
8.4.1	NET 3.1: Remote access applications	50
8.4.2	NET 3.2: Remote access connections	50
8.4.3	NET 3.3: Remote access termination	51
9	SPE 4 – Component security	52
9.1	Purpose.....	52
9.2	COMP 1 – Components and portable media	52
9.2.1	COMP 1.1: Component hardening	52
9.2.2	COMP 1.2: Dedicated portable media.....	53
9.3	COMP 2 – Malware protection.....	53
9.3.1	COMP 2.1: Malware free.....	53
9.3.2	COMP 2.2: Malware protection.....	54
9.3.3	COMP 2.3: Malware protection software validation and installation	54
9.4	COMP 3 – Patch management	55
9.4.1	COMP 3.1: Security patch authenticity/integrity	55
9.4.2	COMP 3.2: Security patch validation and installation	55

9.4.3	COMP 3.3: Security patch status.....	55
9.4.4	COMP 3.4: Security patching retention of security	56
9.4.5	COMP 3.5: Security patch mitigation	56
10	SPE 5 – Protection of data	57
10.1	Purpose.....	57
10.2	DATA 1 – Protection of data.....	57
10.2.1	DATA 1.1: Data classification.....	57
10.2.2	DATA 1.2: Data confidentiality	57
10.2.3	DATA 1.3: Safety system configuration mode	58
10.2.4	DATA 1.4: Data retention policy	59
10.2.5	DATA 1.5: Cryptographic mechanisms	59
10.2.6	DATA 1.6: Key management	60
10.2.7	DATA 1.7: Data Integrity	60
11	SPE 6 – User access control	60
11.1	Purpose.....	60
11.2	USER 1 – Identification and authentication	61
11.2.1	USER 1.1: User identity assignment.....	61
11.2.2	USER 1.2: User identity removal	62
11.2.3	USER 1.3: User identity persistence.....	62
11.2.4	USER 1.4: Access rights assignment	62
11.2.5	USER 1.5: Least privilege	63
11.2.6	USER 1.6: Software service authentication.....	63
11.2.7	USER 1.7: Software services interactive login rights.....	64
11.2.8	USER 1.8: Human user authentication	64
11.2.9	USER 1.9: Multifactor authentication (MFA).....	64
11.2.10	USER 1.10: Mutual authentication.....	65
11.2.11	USER 1.11: Password protection	65
11.2.12	USER 1.12: Shared and disclosed/compromised passwords	66
11.2.13	USER 1.13: User login display information	66
11.2.14	USER 1.14: User login failure displays	66
11.2.15	USER 1.15: Consecutive login failures	67
11.2.16	USER 1.16: Session integrity	67
11.2.17	USER 1.17: Concurrent sessions	67
11.2.18	USER 1.18: Screen lock	68
11.2.19	USER 1.19: Component authentication.....	68
11.3	USER 2 – Authorization and access control	69
11.3.1	USER 2.1: Authorization	69
11.3.2	USER 2.2: Separation of duties.....	69
11.3.3	USER 2.3: Multiple approvals.....	69
11.3.4	USER 2.4: Manual elevation of privileges	70
12	SPE 7 – Event and incident management.....	70
12.1	Purpose.....	70
12.2	EVENT 1 – Event and incident management.....	71
12.2.1	EVENT 1.1: Event detection.....	71

12.2.2	EVENT 1.2: Event reporting	71
12.2.3	EVENT 1.3: Event reporting interfaces	71
12.2.4	EVENT 1.4: Logging	72
12.2.5	EVENT 1.5: Log entries	72
12.2.6	EVENT 1.6: Log access	73
12.2.7	EVENT 1.7: Event analysis	73
12.2.8	EVENT 1.8: Incident handling and response	73
12.2.9	EVENT 1.9: Vulnerability handling.....	74
13	SPE 8 – System integrity and availability	74
13.1	Purpose.....	74
13.2	AVAIL 1 – System availability and intended functionality	75
13.2.1	AVAIL 1.1: Continuity management	75
13.2.2	AVAIL 1.2: Resource availability management	75
13.2.3	AVAIL 1.3: Failure-state.....	75
13.3	AVAIL 2 – Backup/restore/archive	76
13.3.1	AVAIL 2.1: Backup.....	76
13.3.2	AVAIL 2.2: Backup non-interference	76
13.3.3	AVAIL 2.3: Backup verification	76
13.3.4	AVAIL 2.4: Backup media	77
13.3.5	AVAIL 2.5: Backup restoration	77
	Annex A (Informative) Cross references to other standards	79
A.1	Requirements relationship to IEC 62443-2-4.....	79
A.2	Requirements relationship to ISA-62443-3-3.....	83
A.3	Requirements relationship to ISA-62443-4-2.....	87
A.4	Requirements relationship to ISO/IEC 27001:2013	91
A.5	Requirements relationship to the NIST CSF.....	96
	Annex B (Informative) Establishing and maintaining an IACS SP	101
B.1	General	101
B.2	Managing cybersecurity risk	102
B.2.1	Understanding cybersecurity risk	102
B.2.2	Impacts of cybersecurity compromises	102
B.2.3	Risk ranking	102
B.2.4	Cybersecurity attack exposure versus likelihood.....	103
B.3	Elements of a cybersecurity risk assessment/management process	104
B.4	Elements of a cybersecurity risk assessment/management process	105
	Annex C (Informative) Evaluating MLs	107
C.1	Approach to evaluating MLs	107
C.2	Examples of how to evaluate MLs	108
	BIBLIOGRAPHY	110
	Figure 1 – Roles and responsibilities in ISA-62443.....	20
	Figure B.1 – Example of process flow for cybersecurity risk management	105
	Figure B.2 – Levels of protection an asset requires	106

Table 1 – ML levels and descriptions	31
Table 2 – Typical conformity evidence types	34
Table A.1 – ISA-62443-2-4 Cross-References	79
Table A.2 – Cross Reference of ISA-62443-2-1 to ISA-62443-2-4	81
Table A.3 – ISA-62443-3-3 Cross-References	83
Table A.4 – Cross Reference of ISA-62443-2-1 to ISA-62443-3-3	85
Table A.5 – ISA-62443-4-2 Cross-References	87
Table A.6 – Cross Reference of ISA-62443-2-1to ISA-62443-4-2	89
Table A.7 – ISO/IEC 27001:2013 Cross-References.....	91
Table A.8 – ISO/IEC 27001:2013 Cross-References.....	93
Table A.9 – NIST CSF Cross-References.....	96
Table A.10 – Cross Reference of ISA-62443-2-1 to NIST CSF	98
Table B.1 – Example risk levels	103

This page intentionally left blank.

FOREWORD

NOTE The format of this document follows the ISO/IEC requirements discussed in ISO/IEC Directives, Part 2. [1]¹ The ISO/IEC Directives specify the format of this document as well as the use of terms like “shall”, “should”, and “may”.

This document is part of a multipart series that addresses the issue of security for industrial automation and control systems. It has been developed by Working Group 2 of the ISA99 committee in collaboration with IEC TC65/WG10 and ISO/IEC JTC1/SC27.

This document describes the security program (SP) requirements for an industrial automation and control system (IACS) and provides guidance on how to meet each of these requirements.

This second edition cancels and replaces the first edition published in 2009 by ISA and 2010 by IEC. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

- a) revised requirement structure into SP elements (SPEs),
- b) revised requirements to eliminate duplication of an information security management system (ISMS), and
- c) defined a maturity model for evaluating requirements.

¹ Numbers in square brackets refer to the Bibliography.

This page intentionally left blank.

INTRODUCTION

This document is the part of the ISA-62443 series that contains security requirements for industrial automation and control system (IACS) asset owners. In the context of this document, asset owner also includes the operator of the IACS. It has been developed by Working Group 2 of the International Society of Automation (ISA) committee on Security for industrial automation and control systems, ISA99, in collaboration with Working Group 10 of the International Electrotechnical Commission (IEC) Technical Committee 65. Its requirements focus on cybersecurity and allow security capabilities that meet them to be provided as a combination of technical, physical, process and compensating security measures.

Cybersecurity is an increasingly important topic in modern organizations. The term cybersecurity is generally used to describe the set of security measures or practices taken to protect a computer or computer system against unauthorized access or attack. In IACS, the most significant concerns include unwanted access or attacks resulting in the IACS not performing the correct functions in the required timeframe.

A very common engineering approach when faced with a challenging problem is to break the problem into smaller pieces and address each piece in a disciplined manner. This approach is a sound one for addressing cybersecurity risks with IACS. However, a frequent mistake is to deal with cybersecurity one system at a time. Cybersecurity is a much larger challenge that should address all IACS components as well as the policies, procedures, practices and personnel that surround and utilize those IACS. Implementing such a wide-ranging management system can require a cultural change within the organization.

Addressing cybersecurity on an organization-wide basis can seem like a daunting task. There is no simple cookbook for security, nor is there a one-size-fits-all set of security practices. Absolute security can be achievable but is probably undesirable because of the loss of functionality that would be necessary to achieve this near perfect state. Security is a balance of risk versus cost.

Each situation will be different. In some situations, the risk can be related to health, safety and environmental (HSE) factors rather than purely economic impact. The risk can have an unrecoverable consequence rather than a temporary financial setback. Therefore, a predetermined set of mandatory security practices can either be overly restrictive and likely quite costly to implement or be insufficient to address the risk.

This document supports the need to address cybersecurity for an IACS in operation by providing requirements for establishing, implementing, maintaining and continually improving an IACS security program (SP). These requirements, when implemented conscientiously, provide security capabilities whose purpose is to reduce IACS security risks to a tolerable level. These requirements are written to be implementation independent, allowing asset owners to select approaches most suitable to their needs. ISA-62443-3-2 [2]² describes the methodology for addressing cybersecurity risks in an IACS system design and that assists in the identification of risks and the selection of appropriate security requirements and associated capabilities for an IACS SP.

Commercial-off-the-shelf (COTS) products are often not ruggedized or rigorously engineered enough for IACS environments, where they can introduce additional vulnerabilities and threats to the IACS.

² Numbers in square brackets refer to the Bibliography.

When COTS technologies are used in an IACS, they are often configured to meet IACS specific functional needs and operational constraints. For example, security event handling in COTS products may be configured differently for IACS applications than they are for traditional information technology (IT) applications. Typical COTS equipment is designed for environments where the primary objective is the protection of information. In an IACS environment, the primary objectives are the protection of the HSE of the facility and the minimization of the operational and business impact on facility operation. COTS technologies can be applied to IACS applications, but the risks associated with using these technologies need to be understood by the asset owner.

Some organizations can attempt to use pre-existing IT and business cybersecurity solutions to address security for IACS without understanding the consequences. While many of these solutions can be applied to IACS, it is important to apply them correctly to eliminate inadvertent and undesired consequences. For example, in an IACS, availability may have a higher priority than confidentiality, as opposed to typical IT applications.

Asset owners may wish to apply their IACS SP across the organization to address the organization's needs and objectives, security requirements, business and work processes, as well as the organization's size and structure. All of these influencing factors are dynamic and will likely change over time. Thus, the adoption of an IACS SP is a strategic decision for the organization.

The effectiveness of an IACS SP is often enhanced through coordination or integration with the organization's processes and overall information security management system (ISMS). For example, security can be added to the organization's supply chain processes to require security in the design of processes, systems and controls. It is also expected that IACS SP will be scaled in accordance with the needs of the IACS and the organization.

1 Scope

This document specifies asset owner security program (SP) policy and procedure requirements for an industrial automation and control system (IACS) in operation. This document uses the broad definition and scope of what constitutes an IACS as described in ISA-62443-1-1. In the context of this document, asset owner also includes the operator of the IACS.

This document recognizes that the lifespan of an IACS can exceed twenty years, and that many legacy systems contain hardware and software that are no longer supported. Therefore, the SP for most legacy systems addresses only a subset of the requirements defined in this document. For example, if IACS or component software is no longer supported, security patching requirements cannot be met. Similarly, backup software for many older systems is not available for all components of the IACS. This document does not specify that an IACS has these technical requirements. This document states that the asset owner needs to have policies and procedures around these types of requirements. In the case where an asset owner has legacy systems that do not have the native technical capabilities, compensating security measures can be part of the policies and procedures specified in this document.

This document also recognizes that not all requirements specified in this document apply to all IACSs. For example, requirements associated with certain technology (such as, wireless) or functions (such as, remote access) will not apply to IACSs that do not include these technologies or functions. Similarly, not all malware protection requirements apply to systems for which malware protection software is not available for any of their devices. Therefore, this document states that the asset owner needs to identify the IACS security requirements that are applicable to its IACSs in their specific operating environments.

The elements of an IACS SP described in this document define required security capabilities that apply to the secure operation of an IACS. Although the asset owner is ultimately accountable for the secure operation of an IACS, implementation of these security capabilities often includes support from its service providers and product suppliers. For this reason, this document provides guidance for an asset owner when stating security requirements for their service providers and product suppliers, referencing other parts of the ISA-62443 series.

Figure 1 illustrates the roles and responsibilities of the asset owner, service provider(s) and product supplier(s) of an IACS and their relationships to each other and to the Automation Solution. The Automation Solution is a technical solution implementing the control/safety and complementary functions necessary for the IACS. It is composed of hardware and software components that have been installed and configured to operate in the IACS. The IACS is a combination of the Automation Solution and the organizational measures necessary for its design, deployment, operation and maintenance.

Some of these capabilities rely on the appropriate application of integration maintenance capabilities defined in IEC 62443-2-4 [3] and technical security capabilities defined in ISA-62443-3-3 [4] and ISA-62443-4-2 [5].

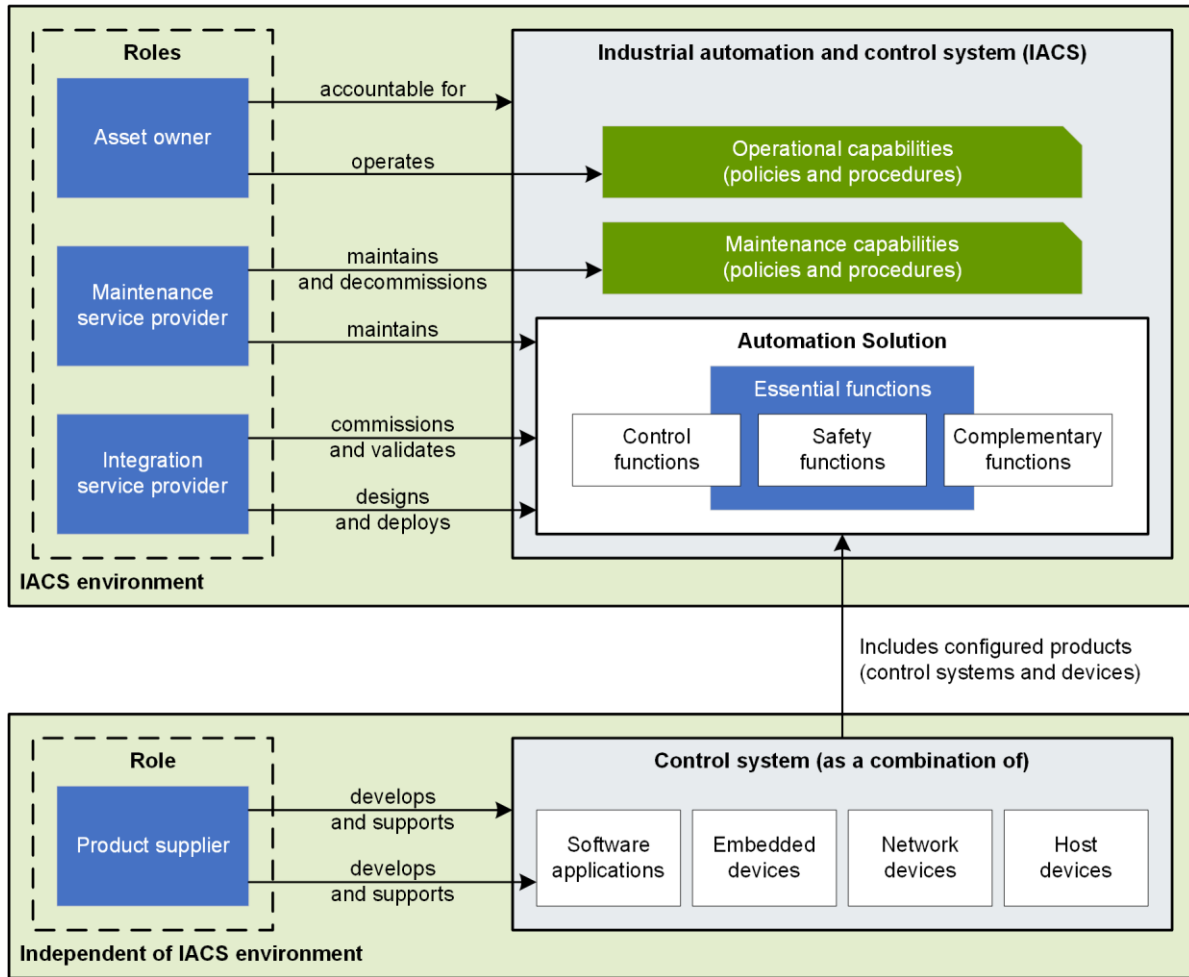


Figure 1 – Roles and responsibilities in ISA-62443

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, Security for industrial automation and control systems,, Part 1-1: Terminology, concepts and models

NOTE This document is currently published by ISA as ANSI/ISA-99.00.01-2007. The document will be renumbered as shown above in the next published edition to remain consistent with its IEC equivalent.

3 Terms, definitions, abbreviated terms, acronyms and conventions

3.1 Terms and definitions

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>

3.1.1

access right

permission to access system resources or privilege to execute system functions

Note to entry: Permissions are generally rights to access resources such as data and executable files, while privileges are generally rights to execute function calls provided by the operating system (OS).

3.1.2

asset owner

organizational role ultimately accountable for one or more IACS

Note 1 to entry: Used in place of the generic word end user to provide differentiation.

Note 2 to entry: In the context of this document, asset owner also includes the operator of the IACS.

[SOURCE ISA-62443-3-3-2013, 3.1.2, modified – changed in definition ‘individual or company responsible’ into ‘organizational role ultimately accountable’ to reflect role; in Note 1 to entry changed ‘The term “asset owner” is used’ into ‘Used’; removed Note 2 to entry; in Note 3 to entry changed ‘this standard, an asset owner’ into ‘this document, asset owner’]

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 document.

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 (for example, 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 can be comprised of components from multiple suppliers, including the product supplier of the control system.

3.1.4

compensating security measure

security measure employed in lieu of or in addition to inherent security capabilities to satisfy one or more security requirements

EXAMPLE 1 (Component-level) A locked cabinet around a controller that does not have sufficient cyber access control security measures.

EXAMPLE 2 (Control system/zone-level) Physical access control (guards, gates and guns) to protect a control room to restrict access to a group of known personnel to compensate for the technical requirement for personnel to be uniquely identified by the IACS.

EXAMPLE 3 (Component-level) A product supplier’s programmable logic controller (PLC) cannot meet the access control capabilities from an asset owner, so the product supplier puts a firewall in front of the PLC and sells it as a system.

3.1.5**consultant**

subcontractor that provides expert advice or guidance to their clients, such as product suppliers, integration and maintenance service providers and asset owners

3.1.6**device**

asset incorporating one or more processors with the capability of sending or receiving data/control to or from another asset

EXAMPLES controllers, human-machine interfaces (HMIs), PLCs, remote terminal units (RTUs), transmitters, actuators, valves, network switches, etc.

3.1.7**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

3.1.8**portable media**

portable devices that contain data storage capabilities that can be used to physically copy data from one piece of equipment and transfer it to another

Note 1 to entry: Types of portable media include but are not limited to, compact disc (CD) / digital versatile disc (DVD) / Blu-ray media, universal serial bus (USB) memory devices, smart phones, flash memory, solid state disks, hard drives, handhelds and portable computers.

Note 2 to entry: The term “removable media” is another term that is often used for “portable media”.

3.1.9**product supplier**

organizational role responsible for the manufacture and support of IACS hardware and/or software products

Note 1 to entry: This term is used in place of the generic word “vendor” to provide differentiation.

3.1.10**security capability**

technology or procedural measure, feature or mechanism that can be used to provide protection against cyber and physical security attacks

Note 1 to entry: Security capabilities are typically implemented through some combination of technology and procedural means. The term “countermeasure” is often used to describe the implementation of “security capability”.

Note 2 to entry: The term “control” is also used to describe this concept in some contexts. The term “security capability” has been chosen for this document to avoid confusion with the word “control” in the context of “process control”.

3.1.11**security compromise**

violation of the security of a system such that an unauthorized (1) disclosure or modification of information, (2) action/execution of functions or (3) denial of service (DoS) could possibly have occurred

Note 1 to entry: A security compromise represents a breach of the security of a system or an infraction of its security policies. It is independent of impact or potential impact to the system.

[SOURCE IEC 62443-2-4:2023, 3.1.20, modified – changed in definition “(2) denial of service could possibly have occurred” into “(2) action/execution of functions or (3) denial of service (DoS) could possibly have occurred”]

3.1.12

security incident

security compromise that is of some significance to the asset owner or failed attempt to compromise the system whose result could have been of some significance to the asset owner

Note 1 to entry: The term “of some significance” is relative to the environment in which the security compromise is detected. For example, the same compromise can be declared as a security incident in one environment and not in another. Triage activities are often used by asset owners to evaluate security compromises and identify those that are significant enough to be considered incidents.

Note 2 to entry: In some environments, failed attempts to compromise the system, such as failed login attempts, are considered significant enough to be classified as security incidents.

[SOURCE IEC 62443-2-4:2023, 3.1.21]

3.1.13

security management system

SMS

set of interrelated or interacting elements of an organization to establish security policies and objectives and a set of systematic processes to achieve those objectives

Note 1 to entry: This definition is based on the ISO/IEC 27000 [6] definition of “management system” and its description in ISO/IEC 27000, 3.41.

3.1.14

security patch

incremental software change in order to address a security vulnerability, a bug, reliability or operability issue (update) or add a new feature (upgrade)

Note 1 to entry: For the purpose of this definition, firmware is considered software.

Note 2 to entry: Software patches can address known or potential vulnerabilities, or simply improve the security of the software component, including its reliable operation.

3.1.15

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 62443-2-4:2023, 3.1.23, modified – Added SP; in Note 1 to entry replaced “security program” with SP, replaced “service providers” with “asset owners” and added “This can include technical, process, physical and compensating security measures used to reduce the cybersecurity attack surface.”]

3.1.16

service provider

organizational role responsible for providing services and associated supplies for the IACS in accordance with an agreement with the asset owner

Note 1 to entry: This term is used in place of the generic word “vendor” to provide differentiation.

3.1.17

software service

software program that is installed and managed by infrastructure software instead of by or on behalf of a logged-on user, typically without a user interface of its own

Note 1 to entry: Some OSs allow logged-on users with elevated privileges to start/stop software services.

3.1.18

tolerable risk

level of risk deemed acceptable to an organization

Note 1 to entry: Organizations should include consideration of legal requirements when establishing tolerable risk. Additional guidance on establishing tolerable risk can be found in ISO 31000 [7] and NIST SP 800-39 [8].

Note 2 to entry: ISA-62443-3-2 provides guidance for establishing tolerable risk.

[SOURCE ISA-62443-3-2, 3.1.22, modified to add Note 2 to entry]

3.2 Abbreviated terms and acronyms

This subclause defines the abbreviated terms and acronyms used in this document.

ANIMA	Autonomic Network Integrated Model and Approach ³
ANSI	American National Standards Institute
API	Application programming interface
BCP	Business continuity plan
BOOTP	Bootstrap protocol
BRSKI	Bootstrapping of a remote secure key infrastructure ³
BSIMM	Building Security In Maturity Model
C2M2	Cybersecurity Capability Maturity Model ⁴
CD	Compact disc
CDA	Critical digital asset
CSF	Cybersecurity Framework ⁵
CIS	Center for Internet Security
CMMC	Cybersecurity Maturity Model Certification ⁶
CMMI	Capability Maturity Model Integration
CMMI-SVC	CMMI for Services
CONOPS	Concept of operations
COTS	Commercial-off-the-shelf

³ IETF

⁴ US DOE

⁵ NIST

⁶ US DOD

DA	Digital asset
DES	Data Encryption Standard
DHCP	Dynamic host configuration protocol
DMZ	Demilitarized zone
DOD	Department of Defense ⁷
DOE	Department of Energy ⁷
DoS	Denial of service
DRP	Disaster recovery plan
DVD	Digital versatile disc
EAP	Extensible Authentication Protocol ³
GPS	Global positioning system
HMI	Human-machine interface
HSE	Health, safety and environment
IACS	Industrial automation and control system(s)
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IIS	Internet Information Services ⁸
IP	Internet protocol
ISA	International Society of Automation
ISMS	Information security management system
ISO	International Organization for Standardization
IT	Information technology
MFA	Multifactor authentication
ML	Maturity level
NIST	National Institute of Standards and Technology ⁷
NTP	Network time protocol
OPC	Open Platform Communications
OS	Operating system
PII	Personally identifiable information
PIN	Personal identification number
PLC	Programmable logic controller
RBAC	Role-based access control
RF	Radio frequency
RFC	Request for Comment ³

⁷ US

⁸ Microsoft

RFQ	Request for quote
RTU	Remote terminal unit
SI	International System of Units
SL	Security level
SL-T	Target SL
SP	Security program
SPE	SP elements
SPR	Security protection rating
SPS	Security protection scheme
SSID	Service set identifier
TCP	Transmission control protocol
UAC	User account control ⁹
UDP	User datagram protocol
USB	Universal serial bus
VPN	Virtual private network

3.3 Conventions

A requirement without qualifier is the same as that requirement with a BR (Basic Requirement) qualifier, for example ORG 1.1 and ORG 1.1 BR are the same requirement.

A requirement with a leading 0 in its numerical fields is the same as that requirement without a leading 0 in its numerical fields, for example SR 2.03 and SR 2.3 are the same requirement.

The above conventions accommodate the different ways the requirements are specified in other ISA-62443 parts.

The term “Automation Solution” is used as a proper noun (and therefore capitalized) in this document to prevent confusion with other uses of this term.

4 Concepts

4.1 Use of this document

4.1.1 Applicable roles

This document primarily applies to the asset owner role, and to a lesser degree, to service provider and product supplier roles (see Figure 1). Organizations who are accountable for the IACS are considered asset owners by the ISA-62443 series. Organizations responsible for the development and support of the hardware and software used in IACS fulfill the product supplier role. Organizations that provide integration services for the IACS fulfill the integration service provider

⁹ Microsoft®. This trade name is provided for reasons of public interest or public safety. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC.

role, while those that provide maintenance services fulfill the maintenance service provider role. These roles and responsibilities are depicted in Figure 1.

It is not uncommon for the organization acting as the asset owner to perform some or all aspects of the integration or maintenance service provider roles, and also perform some or all aspects of the product supplier role for some components of the IACS. In these cases, subclauses 4.1.2 and 4.1.3 will apply to the asset owner organization.

In other cases, the asset owner may contract with one or more product suppliers and/or service providers to deploy and maintain the IACS. In these cases, these organizations may act as one or more of the integration service provider, maintenance service provider or product supplier roles.

Similarly, part or all of a facility may be operated by an entity other than the asset owner. In all cases, the requirements specified by this document apply to the asset owner. The asset owner may have a supply chain program that contains security requirements derived from this document for product suppliers and service providers.

4.1.2 Use of this document by asset owners

4.1.2.1 Risk mitigation

This document defines requirements for IACS SPs of asset owners. In general, an SP consists of defining, implementing and maintaining process, personnel and technology-based capabilities that are intended to reduce the cybersecurity risk of an IACS.

The primary purpose for each of the SP requirements in this document is to mitigate risk. However, risk reduction can take many forms, such as reduction of the likelihood of an incident, reduction of the impact of an incident, reducing the timeline to recover from an incident, and others. In many cases, an SP requirement reduces the overall risk in multiple ways.

The requirements are specified in an implementation independent fashion, allowing a variety of implementations, and allowing users of this document to select a combination of architectural approaches (for example, the use of security zones), policies, procedures and technologies that are most appropriate for their applications.

ISA-62443-3-2 [2] describes a methodology for addressing cybersecurity risks in an IACS Automation Solution design, including the use of security levels (SLs) and security zones.

An IACS SP is typically specific to an individual IACS, of which the facility can have more than one. When there is more than one, it is recommended that a single high-level, facility-level SP be defined whose requirements cascade down as needed to individual IACS SPs. Each IACS SP is dedicated to the availability, integrity and confidentiality of the specific production resources of its IACS, including controllers, field devices and other embedded devices, as well as protecting trade secrets and other confidential information of the IACS.

An IACS SP should be compatible with other IACS SPs at the facility, but this is not always practical or achievable since the technology and risks associated with one IACS can be significantly different than those of another IACS.

IACS SPs are also expected to supplement an asset owner organization's information security management system (ISMS) to provide coordinated operational and information security for the site. ISMS requirements generally do not specifically address all of the security and operational needs of an IACS. This document, along with related parts of the ISA-62443 series, defines the

requirements needed to ensure the operational and informational security of an IACS throughout its lifecycle.

Where practical, IACS SPs should be compatible with the organization's ISMS, but complete consistency with the ISMS is typically not possible due to conflicting objectives of information technology (IT) and IACS systems, and in particular, the essential constraints associated with availability and performance of production facilities. In addition, some of the informational security requirements that apply to protection of the IACS IT aspects can be implemented differently for the IT system and an IACS.

NOTE Alignment of the ISMSs and IACS SPs can be improved by alignment of security goals and objectives between the two systems, and by formally documenting their similarities and differences.

For example, patching policies can be different between IACS SPs and ISMSs as a result of the differences in availability requirements between IACS operator stations and ISMS desktop workstations. Operational constraints, such as this, will typically result in different sets of policies and procedures for IACS SPs and ISMSs.

Since IACSs are a combination of personnel, hardware and software, and processes, SPs of asset owners compliant with this document are composed of:

- a) organizational capabilities that:
 - 1) include an ISMS that typically defines organization-wide policies and practices for IT systems, and
 - 2) support coordination between the IACS and the IT infrastructure in its environment,
- b) technical security capabilities implemented in hardware and software components of the Automation Solution of the IACS (see Figure 1), and
- c) security-related processes, used to securely deploy, configure and operate the IACS, and to maintain its technical security capabilities.

4.1.2.2 SP implementation

This document provides IACS asset owners with a framework to develop and evolve their SPs. Implementing an effective SP for an IACS involves defining and executing comprehensive capabilities that:

- a) address all aspects of security risk management, from identification of programmatic objectives to day-to-day operation, and
- b) include ongoing auditing for program compliance and improvement.

Organizational commitment from top to bottom is essential for IACS SP success. Security of an IACS is a responsibility shared by all members of the organization and their contractors/consultants, and integration of security into their daily activities allows the organization to function more smoothly and succeed in protecting the IACS. SPs based on this document are expected to vary widely depending upon the asset owner's organization and industry. Application of this document to an asset owner's SP begins with determining which of the requirements defined in this document are applicable. Requirements are often determined to be applicable based on the architecture and characteristics of the IACS, the environment in which the IACS operates and the security risks associated with it (see Annex B and ISA-62443-3-2 for more information on management of IACS security risks).

For each applicable requirement, asset owners should implement the appropriate combination of technical and process-oriented capabilities. Technical capabilities are features of the IACS and its

components, and process-oriented capabilities are organizational processes used to integrate/deploy the IACS, operate it and maintain it.

Cross-references are provided to ISA-62443-3-3 and ISA-62443-4-2 for technical capabilities and to IEC 62443-2-4 for integration and maintenance capabilities. These cross-referenced capabilities can be used by asset owners when determining the technical and process-oriented capabilities they will implement and for specifying security requirements for their product suppliers and service providers.

It could be impossible or impractical for an asset owner to establish and implement an SP that meets all applicable requirements at once. Therefore, asset owners may, if necessary, develop a phased approach to evolve their SP. In such cases, the initial emphasis should be on effectively managing the highest risks.

This document also recognizes that it can be desirable for asset owners to implement an SP that meets the requirements specified in this document in ways that are consistent with other security specifications. Therefore, Annex A reports cross-references to and from each requirement of this document with requirements in related external references, in particular with ISO/IEC 27001 [9] and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) [10]. Using these cross-references, the asset owner can harmonize with related external requirements when implementing each of its SP capabilities.

NOTE In the context of an IACS, all references in ISO/IEC 27001 to “information management” refer to the IACS.

Some legacy IACS can preclude direct implementation of specific requirements or subsets of applicable requirements. In these instances, compensating security measures should be implemented where possible.

4.1.2.3 Organizational interfaces

Although the asset owner is ultimately accountable for the operation of the IACS and processes controlled by the IACS, associated responsibilities are often fulfilled with the support of service providers and product suppliers. The respective legal, operational and technical roles and responsibilities for these entities are generally defined in contracts and procurement documents, such as request for quotes (RFQs) and purchase orders. Ideally, security requirements are included in these documents.

When the service provider or product supplier is part of the asset owner’s organization, there might not be such a contract, but the security requirements for products and integration/maintenance processes are typically still specified for the IACS.

This document provides in Annex A cross-references to and from each requirement of this document with service provider and product supplier requirements specified in IEC 62443-2-4, ISA-62443-3-3 and ISA-62443-4-2. Asset owners can use these cross-references to assist in the development of security requirements for service provider and product supplier procurement documents. These referenced documents and the requirements cross-references included in Annex A of this document can assist asset owners, service providers and product suppliers to agree on a consistent set of requirements during procurement.

4.1.3 Use of this document by service providers and product suppliers

As described in 4.1.2.3, IEC 62443-2-4, ISA-62443-3-3 and ISA-62443-4-2 define security requirements for products and services procured by asset owners. Since these requirements are

cross-referenced to this document's requirements in Annex A, this document can provide a useful context to service providers and product suppliers.

4.2 Maturity level (ML) definitions

The SP requirements defined in this document beginning in 5.3 have been specified to be implementation independent. This is done to allow the asset owner latitude in applying this document while meeting the needs of its organization.

To support implementation independence for process security measures that meet these requirements, a range of MLs from entry level processes to refined and improved processes is defined in Table 1. MLs apply independently to SP requirements, and the asset owner should select the most appropriate ML for a requirement based on risk management goals (see ISA-62443-3-2). While the asset owner can have policies and procedures that satisfy multiple SP requirements, each SP requirement should be evaluated independently. See Annex C for more information about evaluating MLs.

Additionally, since some asset owners could need to use a phased approach to evolve their SPs, a range of program MLs can prove helpful in the planning and scheduling of phases. Note that other parts of ISA-62443 that define requirements for process security measures, such as IEC 62443-2-4 and ISA-62443-4-1 [11], also incorporate ML.

This document's range of MLs is defined by a model that is composed of maturity benchmarks for implementation of process security measures. The benchmarks for each ML are shown in Table 1. The MLs are based on the Capability Maturity Model Integration (CMMI) for Services (CMMI-SVC) model [12]. Table 1 shows the relationship to the CMMI-SVC in the "Description/comparison to CMMI-SVC" column.

Table 1 – ML levels and descriptions

Level	CMMI-SVC	This document	Description/comparison to CMMI-SVC
1	Initial	Initial	At this level, the models are fundamentally the same. Processes are performed in an ad-hoc and often undocumented (or not fully documented) manner. As a result, consistency over time can be difficult to show. NOTE: “Documented” in this context refers to the procedure followed in performing this service (for example, detailed instructions to service provider personnel), not to the results of performing the process. In most IACS, changes resulting from the performance of a procedural process are often documented.
2	Managed	Managed	At this level, the models are fundamentally the same, with the exception that this document recognizes that there can be a significant delay between defining a process and executing/practicing it. Therefore, the execution related aspects of the CMMI-SVC Level 2 are deferred to Level 3. At this level, documentation exists that describes how to manage the delivery and performance of the capability. This documentation can be in the form of written procedures or written training programs for performing the capability. The discipline reflected by ML 2 helps to ensure that practices are repeatable, even during times of stress. When these practices are in place, their execution will be performed and managed according to their documented plans.
3	Defined	Defined / Practiced	At this level, the models are fundamentally the same, with the exception that the execution related aspects of the CMMI-SVC Level 2 are included here. Therefore, a process at Level 3 is a Level 2 process that is being practiced on the IACS. The performance of a Level 3 practice can be shown to be repeatable over time within the IACS.
4	Quantitatively Managed	Improving	At this level, the “Quantitatively Managed” and “Optimizing” CMMI-SVC levels are combined. Using suitable process metrics, the effectiveness or performance improvements of the process or both, can be demonstrated. This results in an SP that improves the process through technological/procedural/ management changes.
	Optimizing		

Beginning with ML 2, processes are required to be documented. This includes documented policies and procedures as well as documented training for personnel. As a consequence, the SP requirements specified in this document do not state the need for documentation because the ML 2 and above require documentation.

Within this maturity model, each level is progressively more advanced than the previous level and applies independently for each requirement. MLs are a part of the conformance assessment process, so asset owners are required to identify whether they meet each requirement, and if so, the ML associated with their implementation of each requirement or group of requirements.

NOTE It is intended for evolution of an SP, that over time and for a specific requirement, a process will evolve to higher levels as the organization gains proficiency in meeting the requirement.

4.3 Security levels (SLs)

SLs for IACS represent the relative strength of security capabilities defined for the IACS Automation Solution in ISA-62443-3-3 and for components in ISA-62443-4-2.

This document does not describe the methodologies for defining zones and conduits, or determining SLs for zones, conduits and components. Instead, those methodologies are defined in ISA-62443-3-2 for zones and conduits, and ISA-62443-4-2 for components. This document defines the requirements for the overall SP within the organization to manage risk on an ongoing basis, via implementing and maintaining process, personnel and technology-based capabilities.

To correlate SP requirements in this document with target SLs (SL-Ts) for zones, conduits and components, the asset owner can use the cross-references to ISA-62443-3-3 and ISA-62443-4-2 that are provided with the SP requirement to understand the requirements/requirements enhancements associated with the SL-T from those documents.

For example, this document can state an SP should have a process to ensure proper authentication is ensured across the organization. However, to address confidence in the implementation of user authentication capabilities, the asset owner should request its product suppliers to show the product in question was developed using ISA-62443-4-1 compliant processes, and the product capabilities are compliant with relevant ISA-62443-4-2 requirements. Similarly, to address confidence in the installation, configuration and maintenance of these user authentication capabilities, the asset owner would request its service providers to use processes for these capabilities that are compliant to the cross-referenced IEC 62443-2-4 requirements, SP.03.07 RE(1) and SP.09.xx.

4.4 Requirements definitions

4.4.1 Requirements organization

Subclause 5.3 and Clauses 6 through 13 define the selection methodology and individual requirements for asset owner SPs. These requirements have been specified to be implementation independent, allowing the asset owner to select the most suitable implementation for its IACS.

Requirements are organized into SPEs that represent top level activities of the SP, such as organizational security measures, configuration management, network and communications security and component security. SPEs are composed of requirements for a combination of organizational and technical security controls that can be used to implement a defense-in-depth strategy for the IACS.

4.4.2 Requirements cross-references

To aid the asset owner's use of this document, the requirements have been cross-referenced to other parts of the ISA-62443 series and other security specifications that include system and component requirements. This cross-reference is provided to support activities spanning documents in the series, such as the integration of the asset owner's SP with its ISMS and with its supply chain processes as they relate to security.

These cross-references support asset owner efforts to implement the requirements of this document consistently with the other parts of the ISA-62443 series and with the other referenced specifications. Blank entries in these cross-references mean that there is no corresponding requirement in the cross-referenced document. These cross-references are reported in Annex A.

4.4.3 Requirement conventions

Some of the requirements definitions contain the phrase: "commonly accepted". This phrase is used when the required capability implementation is dependent on the current state of the art, and the state of the art at the time of conformance assessment is used to determine whether the requirement has been met. For example, when the Data Encryption Standard (DES) was

developed, it had no known vulnerabilities, but since then vulnerabilities have been discovered and it is no longer appropriate for use in IACSs. The “Rationale and supplemental guidance” subclause of each requirement provides additional explanation of the use of this phrase.

5 Conformance and assessment

5.1 Overview

The formal definitions for terms like conformance, conformity and assessment come from other sources, such as ISO/IEC 17000 [13]. The ISA-62443 series provides guidance for conformity and assessments for various roles (see 4.1.1). This guidance is intended to assist the various roles in understanding the conformance and assessment process and is not intended to supersede any of the definitions provided in ISO/IEC 17000.

Conformance or conformity with the ISA-62443 series means the affected role has evaluated, and where applicable applied and documented, all methods identified in each requirement of the applicable series part thereby mitigating security risks and identifying the conformity for all identified processes with the necessary supporting evidence.

Assessment means the affected role has performed specific measurement of conformity with the requirements through use of some type of verification process or specific validation process. Those validated processes can be applied through an internal organization process or the use of a third-party identified process compliant with the ISA-62443 series, and also are verified by supplying the necessary supporting evidence.

Conformity assessments can be self-assessments performed by the asset owner, service provider or product supplier roles using internal processes, or assessments can be performed by a qualified, independent third-party. When independent third-party assessments are used, it is important to note that credentialing processes of the third-party are wide and varied and are outside the scope of this document,

Assessment processes themselves are also outside the scope of this document.

Asset owners may have their “as-deployed” control systems, IACS or Automation Solutions assessed for conformance to ISA-62443-3-3 and their “as-provided” integration and maintenance services assessed for conformance to IEC 62443-2-4. These assessments would verify conformance at the time the control system was assessed, or the services were provided. Supplementing these assessments are evaluations that combine security levels and organizational MLs to indicate the composite SP protection provided to the IACS.

Asset owners may assess their IACS and Automation Solutions for conformance to this document, to verify they have an SP in place to sustain a security posture for the IACS which includes all technical components and organizational processes. It is also desirable for the IACS or Automation Solution to use security certified products in the design that are correctly deployed and maintained by certified service providers.

Product suppliers providing products to an asset owner may have their products and development processes assessed for conformance to ISA-62443-3-3, ISA-62443-4-1 and ISA-62443-4-2.

Service providers providing services to an asset owner may have their integration and maintenance services assessed for conformance to IEC 62443-2-4.

5.2 Conformity evidence

Proof of conformity and conformance methods can be provided in many forms as shown in Table 2. Most requirements identify supporting evidence by identifying the specific methods that include, but are not limited to:

- verifying the use,
- capability and configuration of technology,
- their supporting processes, and
- validation through testing of capabilities.

Table 2 – Typical conformity evidence types

Evidence type	Description
Configuration records	Records that show configuration settings, component inventories, patch records, etc.
Legal documents	Contracts and related documents, including subcontractor agreements, signed employee statements, background checks, asset owner approvals, etc.
Organization charts, position descriptions and personnel records	Job related documentation that describes customer roles, including personnel requirements (for example, expertise/experience), job responsibilities and organizational relationships. Also, records that show who was assigned/de-assigned to these positions (for example, to Automation Solution activities).
Product documentation	Internal and external documents that describe the product, such as design documents, product data sheets, knowledge-based articles and network scanning tools.
Screen shots	Screen captures of user interfaces.
Security assessments	Reports that document security-related issues, such as risks, security incidents and vulnerabilities.
Security testing documentation	Internal and external documents that describe the security tests/results used to verify security aspects of the product or installation of the product.
Service policies and procedures	Internal customer documentation that describes policies and procedures used by customer personnel to install, configure, harden and maintain the Automation Solution.
Security-related activity documentation/checklists	Documentation, such as checklists, that records the results of security-related activities, such as risk assessments, threat models, reviews, architecture drawings, test results, spreadsheets, etc.
Automated reports	Reports generated by the IACS.
Training materials/course descriptions	Documents that describe how training is conducted and documents that show the content of the training course, such as a syllabus or course overview.
Training records	Documents that show completion of training. These documents typically show who was trained, when they were trained and the course names. These can take the form of course rosters, course diplomas, human resource records, etc.
User documentation	User manuals, instructions, etc.. that describe to the user how to configure, operate, maintain or otherwise interact with the IACS and its products and services.
Testing results	Any and all tests, performed by a qualified person having the appropriate training, on a documented configuration of components, IACS and Automation Solution that verify specifically identified requirements conformance.

5.3 Requirements evaluation and profiles

5.3.1 Overview

In preparation for a conformance assessment, asset owners need to evaluate each requirement in an applicable part of the series for its guidance in mitigating the risk addressed by the requirement.

In the event a role determines through evaluation any requirement may not apply, it is the asset owner's responsibility to justify why a requirement does not apply and provide supporting evidence stating specifically why the requirement does not apply including specifically how that security risk has been otherwise mitigated through other security measures.

5.3.2 Evaluation of risk to requirements

The determination of the cybersecurity risks to be mitigated (see 4.1.2.1 and 6.3.1, ORG 2.1: Security risk mitigation) is typically performed as part of the asset owner's risk management process in ISA-62443-3-2. This process should incorporate "risk response" activities as described in ISA-62443-1-1 and ISA-62443-3-2, which are responsible for identifying and dispositioning risks. Completing the risk management process in ISA-62443-3-2 is critical to the security of the IACS even if a conformance assessment is not performed.

Requirements then are applied based on risk mitigation and apply to all circumstances where identified risks need to be mitigated to a tolerable level, and conversely, if requirements may not apply where risks have evidence to prove the risk can be at a tolerable level.

Each requirement is selected based on risk mitigation and interpreted in the context of tolerable risk; that is, meeting the requirement means that the asset owner has either mitigated or accepted the risks associated with the requirement with supporting evidence.

If the asset owner is not prepared to accept the risks, then the requirement is not met.

5.3.3 Profiles

It can be necessary for some industries and verticals to align the requirements in this and other ISA-62443 documents to industry/vertical-specific concepts and terminology. In order to provide additional flexibility in the application of the standards series, IEC TS 62443-1-5 [14] describes a method for one or more organizations to create a common profile of the ISA-62443 standards series. A profile allows an interested party (organization, group, sector, conformity assessment body, etc.) to select a subset of requirements from one or more standards in the ISA-62443 series, provide a contextual mapping for those requirements (for example, to an industry/vertical) and specify a minimum security or maturity level for selected requirements.

Published profiles can be used as a common basis of assessment against a subset or industry/vertical-specific mapping of the requirements in the ISA-62443 standards series. They support interested parties during conformity assessment activities, to achieve comparability of assessed ISA-62443 requirements.

5.3.4 Conformity assessment for the Asset Owner role

In preparation for a conformity assessment, asset owners can select the requirements that are to be assessed based on:

- a) a security profile to which the asset owner claims conformance; or
- b) the outcome of an IACS specific cyber security risk assessment and identification of applicable requirements necessary to reduce risks to a tolerable level.

A requirement might not be applicable because, for example, the IACS does not contain components/technology, such as wireless and safety systems addressed by the requirement.

Risk management is critical to the security of the IACS even if a conformity assessment is not performed.