



**Standards**

- Certification
- Education & Training
- Publishing
- Conferences & Exhibits

*Setting the Standard for Automation™*

AMERICAN NATIONAL STANDARD

**ANSI/ISA-62443-3-2-2020**

# **Security for industrial automation and control systems, Part 3-2: Security risk assessment for system design**

**Approved August 11, 2020**

**NOTICE OF COPYRIGHT**

This is a copyrighted 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 ISA's license to that person. It may not be provided to any other person in print, electronic, or any other form. Violations of ISA's copyright will be prosecuted to the fullest extent of the law and may result in substantial civil and criminal penalties.

**ANSI/ISA-62443-3-2-2020**

Security for industrial automation and control systems,  
Part 3-2: Security risk assessment for system design

ISBN: 978-1-64331-116-6

Copyright © 2020 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

67 T.W. Alexander Drive

P. O. Box 12277

Research Triangle Park, NC 27709 USA

## PREFACE

This preface, as well as all footnotes and annexes, is included for information purposes and is not part of ANSI/ISA-62443-3-2-2020.

This document has been prepared as part of the service of ISA, the International Society of Automation, toward a goal of uniformity in the field of instrumentation. 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, Standards and Practices Board; ISA; 67 T.W. Alexander Drive; P. O. Box 12277; Research Triangle Park, NC 27709; Telephone (919) 549-8411; Fax (919) 549-8288; E-mail: standards@isa.org.

The ISA Standards and Practices Department is aware of the growing need for attention to the metric system of units in general and the International System of Units (SI) in particular, in the preparation of instrumentation standards. The Department is further aware of the benefits to USA users of ISA standards of incorporating suitable references to the SI (and the metric system) in their business and professional dealings with other countries. Toward this end, this Department will endeavor to introduce SI-acceptable metric units in all new and revised standards, recommended practices and technical reports to the greatest extent possible. Standard for Use of the International System of Units (SI): The Modern Metric System, published by the American Society for Testing and Materials as IEEE/ASTM SI 10-97, and future revisions, will be the reference guide for definitions, symbols, abbreviations, and conversion factors.

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.

**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 standard, 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 standard or a license on reasonable terms and conditions that are free from unfair discrimination.**

**Even if ISA is unaware of any patent covering this Standard, the user is cautioned that implementation of the standard 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 standard. ISA is not responsible for identifying all patents that may require a license before implementation of the standard or for investigating the validity or scope of any patents brought to its attention. The user should carefully investigate relevant patents before using the standard for the user's intended application.**

**However, ISA asks that anyone reviewing this standard who is aware of any patents that may impact implementation of the standard notify the ISA Standards and Practices Department of the patent and its owner.**

**Additionally, the use of this standard may involve hazardous materials, operations or equipment. The standard cannot anticipate all possible applications or address all possible safety issues associated with use in hazardous conditions. The user of this standard 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 standard.**

The following people served as active members of ISA99 Working Group 04, Task Group 03 for the preparation of this document:

<b>Name</b>	<b>Company</b>	<b>Contributor</b>	<b>Reviewer</b>
John Cusimano, TG Chair	aeSolutions	X	
Rahul Bhojani, Former TG Chair	BP	X	
Jens Braband	Siemens	X	
Eric Byres	aDolus Inc.		X
Maarten de Caluwé	The Dow Chemical Company	X	
Eric Cosman	OIT Concepts LLC		X
William J. Cotter	3M Co.		X
Ed Crawford	Chevron		X
Paul Didier	Cisco	X	
Bob Evans	Individual	X	
Jim Gilsinn	Kenexis		X
Andrew Ginter	Waterfall		X
Thomas Good	DuPont		X
Vic Hammond	Argonne National Laboratory		X
Jean-Pierre Hauet	KB Intelligence		X
Dennis Holstein	OPUS Consulting Group		X
Eric Hopp	Rockwell		X
Siv Hilde Houmb	Secure-NOK AS	X	
Dave Johnson	Exida	X	
Joel Langill	AECOM		X
John Lellis	Individual	X	
Suzanne Lightman	NIST	X	
Ken Keiser	E&Y	X	
Pierre Kobes	Siemens	X	
Michael Medoff	Exida		X
Kenny Mesker	Chevron	X	
Johan Nye	ICS Guru LLC		X
Bryan Owen	OSISoft Inc.		X
Dennis Parker	Chevron	X	
Michal Paulski	Accenture	X	
Jeff Potter	Independent Consultant	X	
Judith Rossebo	ABB	X	
Ragnar Schierholz	ABB	X	
Omar Sherin	Q-Cert		X
Kevin Staggs	Honeywell		X
Leon C. Steinocher	Redstone Investors		X
Tatsuaki Takebe	Yokogawa		X
Hal Thomas	Exida		X
Ludwig A. Winkel	Siemens		X

This standard was approved for publication by the ISA Standards and Practices Board on August 3, 2020.

**NAME**

**AFFILIATION**

C. Monchinski, Vice President	Automated Control Concepts Inc.
D. Bartusiak	ExxonMobil Research & Engineering
D. Brandl	BR&L Consulting
P. Brett	Honeywell Inc.
E. Cosman	OIT Concepts, LLC
D. Dunn	Waldemar S. Nelson & Co.
J. Federlein	Federlein & Assoc LLC
B. Fitzpatrick	Wood PLC
J-P Hauet	Hauet.com
D. Lee	Emerson Automation Solutions
G. Lehmann	AECOM
T. McAvinew	Consultant
V. Mezzano	Fluor Corporation
G. Nasby	City of Guelph Water Services
M. Nixon	Emerson Process Management
D. Reed	Rockwell Automation
N. Sands	DuPont Company
H. Sasajima	Fieldcomm Group Inc. Asia-Pacific
H. Storey	Herman Storey Consulting
I. Verhappen	Industrial Automation Networks
D. Visnich	Burns & McDonnell
W. Weidman	Consultant
J. Weiss	Applied Control Solutions LLC
M. Wilkins	Yokogawa UK Ltd.
D. Zetterberg	Chevron Energy Technology Company

This page intentionally left blank.

## CONTENTS

FOREWORD .....	9
INTRODUCTION .....	11
1 Scope .....	13
2 Normative references .....	13
3 Terms, definitions, abbreviated terms, acronyms and conventions .....	13
3.1 Terms and definitions.....	13
3.2 Abbreviated terms and acronyms .....	16
3.3 Conventions.....	17
4 Zone, conduit and risk assessment requirements .....	17
4.1 Overview.....	17
4.2 ZCR 1: Identify the SUC.....	19
4.2.1 ZCR 1.1: Identify the SUC perimeter and access points .....	19
4.3 ZCR 2: Initial cyber security risk assessment .....	19
4.3.1 ZCR 2.1: Perform initial cyber security risk assessment .....	19
4.4 ZCR 3: Partition the SUC into zones and conduits .....	19
4.4.1 Overview.....	19
4.4.2 ZCR 3.1: Establish zones and conduits .....	20
4.4.3 ZCR 3.2: Separate business and IACS assets .....	20
4.4.4 ZCR 3.3: Separate safety related assets .....	20
4.4.5 ZCR 3.4: Separate temporarily connected devices .....	21
4.4.6 ZCR 3.5: Separate wireless devices .....	21
4.4.7 ZCR 3.6: Separate devices connected via external networks .....	21
4.5 ZCR 4: Risk comparison .....	21
4.5.1 Overview .....	21
4.5.2 ZCR 4.1: Compare initial risk to tolerable risk.....	21
4.6 ZCR 5: Perform a detailed cyber security risk assessment .....	22
4.6.1 Overview .....	22
4.6.2 ZCR 5.1: Identify threats .....	23
4.6.3 ZCR 5.2: Identify vulnerabilities.....	24
4.6.4 ZCR 5.3: Determine consequence and impact .....	24
4.6.5 ZCR 5.4: Determine unmitigated likelihood.....	25
4.6.6 ZCR 5.5: Determine unmitigated cyber security risk .....	25
4.6.7 ZCR 5.6: Determine SL-T.....	25
4.6.8 ZCR 5.7: Compare unmitigated risk with tolerable risk.....	26
4.6.9 ZCR 5.8: Identify and evaluate existing countermeasures .....	26
4.6.10 ZCR 5.9: Reevaluate likelihood and impact .....	26
4.6.11 ZCR 5.10: Determine residual risk.....	27
4.6.12 ZCR 5.11: Compare residual risk with tolerable risk .....	27
4.6.13 ZCR 5.12: Identify additional cyber security countermeasures .....	27
4.6.14 ZCR 5.13: Document and communicate results .....	28

4.7	ZCR 6: Document cyber security requirements, assumptions and constraints .....	28
4.7.1	Overview .....	28
4.7.2	ZCR 6.1: Cyber security requirements specification .....	28
4.7.3	ZCR 6.2: SUC description .....	29
4.7.4	ZCR 6.3: Zone and conduit drawings .....	29
4.7.5	ZCR 6.4: Zone and conduit characteristics .....	29
4.7.6	ZCR 6.5: Operating environment assumptions .....	31
4.7.7	ZCR 6.6: Threat environment .....	31
4.7.8	ZCR 6.7: Organizational security policies .....	31
4.7.9	ZCR 6.8: Tolerable risk .....	31
4.7.10	ZCR 6.9: Regulatory requirements .....	32
4.8	ZCR 7: Asset owner approval .....	32
4.8.1	Overview .....	32
4.8.2	ZCR 7.1: Attain asset owner approval .....	32
	Annex A (informative) Security levels .....	33
	Annex B (informative) Risk matrices .....	35
	BIBLIOGRAPHY .....	38
	Figure 1 – Parts of the ISA-62443 series .....	11
	Figure 2 – Workflow diagram outlining the primary steps required to establish zones and conduits, as well as to assess risk .....	18
	Figure 3 – Detailed cyber security risk assessment workflow per zone or conduit .....	23
	Table B.1 – Example of a 3 x 5 risk matrix .....	35
	Table B.2 – Example of likelihood scale .....	35
	Table B.3 – Example of consequence or severity scale .....	36
	Table B.4 – Example of a simple 3 x 3 risk matrix .....	36
	Table B.5 – Example of a 5 x 5 risk matrix .....	37
	Table B.6 – Example of a 3 x 4 matrix .....	37

## 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 04, Task Group 03.

This document prescribes the requirements to perform cyber security risk assessment of an IACS in order to inform the organization of the initial risk, residual risk and target security level (SL-T) for the system under consideration (SUC). The standard also prescribes the requirements to utilize the output of the risk assessment to produce a cyber security requirement specification (CRS) to guide system design.

This page intentionally left blank.

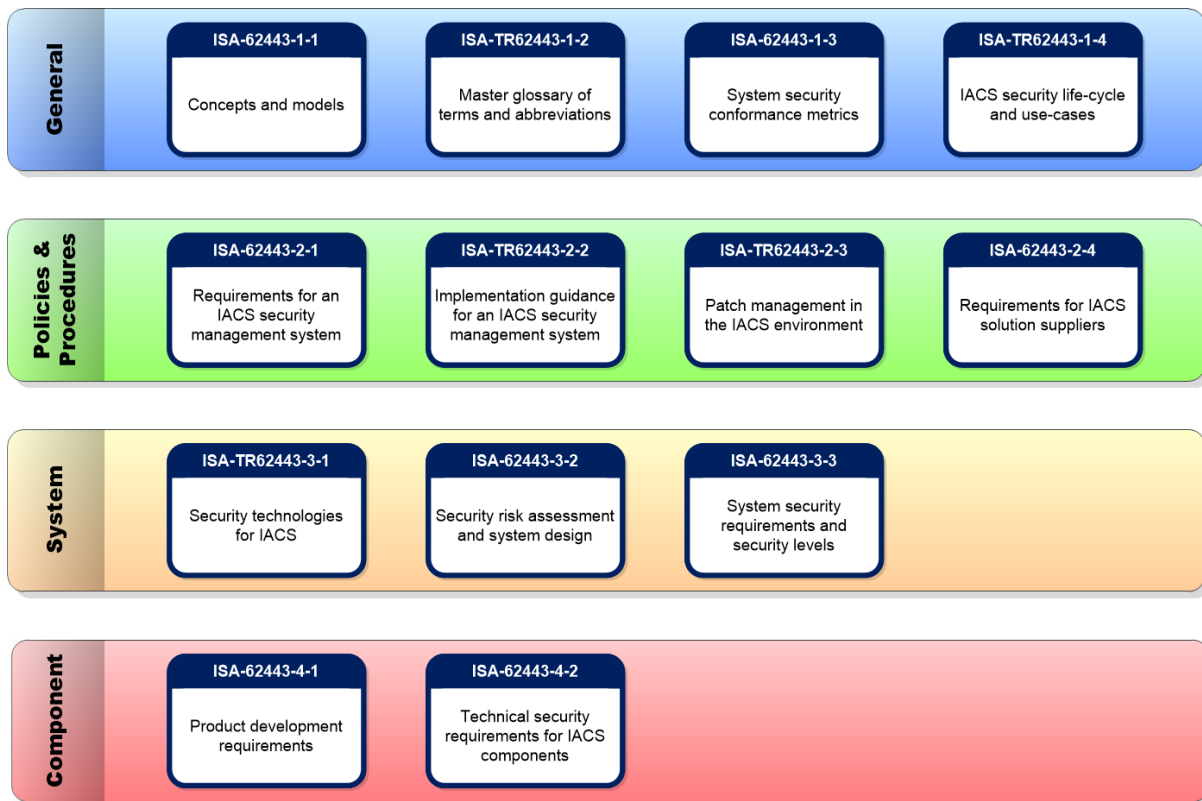
## INTRODUCTION

There is no simple recipe for how to secure an industrial automation and control system (IACS) and there is good reason for this. It is because security is a matter of risk management. Every IACS presents a different risk to the organization depending upon the threats it is exposed to, the likelihood of those threats arising, the inherent vulnerabilities in the system and the consequences if the system were to be compromised. Furthermore, every organization that owns and operates an IACS has a different tolerance for risk.

This document strives to define a set of engineering measures that will guide an organization through the process of assessing the risk of a particular IACS and identifying and applying security countermeasures to reduce that risk to tolerable levels.

A key concept in this document is the application of IACS security zones and conduits. Zones and conduits are introduced in ISA-62443-1-1. Readers are encouraged to familiarize themselves with these concepts prior to reading this document.

Figure 1 illustrates the relationship of the different parts of ISA-62443 that were in existence or planned as of the date of circulation of this document. Those that are normatively referenced are included as normative references and those that are referenced for informational purposes or that are in development are listed in the Bibliography.



**Figure 1 – Parts of the ISA-62443 series**

### Purpose and intended audience

The audience for this document is intended to include the asset owner, system integrator, product supplier, service provider, and compliance authority.

**Usage within other parts of the ISA-62443 series**

This document provides a basis for specifying security countermeasures by aligning the target security levels (SL-Ts) identified in this standard with the required capability security levels (SL-Cs) specified in ISA-62443-3-3.

## 1 Scope

This document establishes requirements for:

- defining a system under consideration (SUC) for an industrial automation and control system (IACS);
- partitioning the SUC into zones and conduits;
- assessing risk for each zone and conduit;
- establishing the target security level (SL-T) for each zone and conduit; and
- documenting the security requirements.

## 2 Normative references

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

ISA-62443-2-1, *Security for industrial automation and control systems Part 2-1: Establishing an industrial automation and control systems security program*

ISA-62443-3-3, *Security for industrial automation and control systems Part 3-3: System security requirements and security levels*

## 3 Terms, definitions, abbreviated terms, acronyms and conventions

### 3.1 Terms and definitions

For the purposes of this document, the following terms and definitions given in ISA-62443-1-2 [1]<sup>1</sup> and the following apply.

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

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

#### 3.1.1

##### **channel**

specific logical or physical communication link between assets

Note 1 to entry: A channel facilitates the establishment of a connection.

#### 3.1.2

##### **compliance authority**

entity with jurisdiction to determine the adequacy of a security assessment or the effectiveness of implementation as specified in a governing document

Note 1 to entry: Examples of compliance authorities include government agencies, regulators, external and internal auditors.

#### 3.1.3

##### **conduit**

logical grouping of communication channels that share common security requirements connecting two or more zones

---

<sup>1</sup> Numbers in brackets indicate references in the Bibliography.