



Standards

Certification

Education & Training

Publishing

Conferences & Exhibits

Setting the Standard for Automation™

AMERICAN NATIONAL STANDARD

ANSI/ISA-62443-4-2-2018

Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components

Approved 13 August 2018

This is a preview. [Click here to purchase the full publication.](#)

ANSI/ISA-62443-4-2-2018

Security for industrial automation and control systems – Part 4-2:
Technical security requirements for IACS components

ISBN: 978-1-64331-025-1

Copyright © 2018 by ISA. All rights reserved. Not for resale. Printed in the United States of America.

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-62443-4-2.

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.

ISA (www.isa.org) is a nonprofit 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 global standards; certifies industry professionals; provides education and training; publishes books and technical articles; hosts conferences and exhibits; and provides networking and career development programs for its 40,000 members and 400,000 customers around the world.

ISA owns Automation.com, a leading online publisher of automation-related content, and is the founding sponsor of The Automation Federation (www.automationfederation.org), an association of nonprofit organizations serving as “The Voice of Automation.” 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 04, Task Group 4 in the preparation of this document:

Name	Company	Contributor	Reviewer
Kevin Staggs, TG Chair	Honeywell Inc.	X	
Dennis Brandl	BR&L Consulting		X
Khaled Brown	Intel Security		X
Eric Byres	Byres Security Consulting.		X
Eric Cosman	OIT Concepts, LLC		X
William Cotter	3M Company		X
Ed Crawford	ProcessControl/SCADA Security		X
John Cusimano	AE Solutions	X	
Maarten de Caluwé	Dow Benelux BV		X
Michael Dransfield	NSA	X	
Mark Fabro	Lofty Perch Inc.		X
Ronald Forrest	Forrest Automation & Technology Solutions LLC		X
Dirk Gebert	Siemens AG	X	
Jim Gilsinn	Kenexis Consulting	X	
Thomas Good	ICS Security Consultant		X
Evan Hand	Consultant		X
Vic Hammond	Argonne National Laboratory		X
Mark Heard	TMD Consulting		X
Dennis Holstein	OPUS Consulting Group		X
Bruce Honda	Weyerhaeuser		X
Charles Hoover	Emerson	X	
Eric Hopp	Rockwell Automation		X
Bob Huba	Tall Corn Security Consulting		X
Andrew Kling	Schneider Electric	X	
Pierre Kobes	Siemens AG	X	
Nate Kube	Consultant	X	
Joel Langill	AECOM		X

Suzanne Lightman	NIST		X
Charles Mastromonico	Westinghouse Savannah River Co.		X
Mike Medoff	Exida		X
Roberto Minicucci	GE Oil and Gas	X	
Ajay Mishra	Schneider Electric	X	
Jason Moore	Xilinx Inc.	X	
Alex Nicoll	Rockwell Automation	X	
Johan Nye	Consultant	X	
Bryan Owen	OSISoft Inc		X
Tom Phinney	Consultant		X
Jeff Potter	Consultant	X	
Bob Radvanovsky	Infracritical		X
Judith Rossebo	ABB AS	X	
Ragnar Schierholz	ABB AG	X	
Omar Sherin	Q-Cert		X
Leon Steinocher	Redstone Investors		X
Herman Storey	Herman Storey Consulting		X
Michele Struvay	NXP Semiconductors	X	
Tatsuaki Takebe	KPMG Consulting Co., Ltd.		X
Bradley Taylor	The Catholic University of America		X
Zachary Tudor	Idaho National Laboratory		X
Joseph Weiss	Applied Control Solutions LLC		X
Ludwig Winkel	Siemens AG		X

This standard was approved for publication by the ISA Standards and Practices Board on 12 July 2018.

NAME	COMPANY
M. Wilkins, Vice President	Yokogawa UK Ltd.
D. Bartusiak	ExxonMobil Research & Engineering
D. Brandl	BR&L Consulting
P. Brett	Honeywell Inc.
E. Cosman	OIT Concepts, LLC
D. Dunn	T.F. Hudgins, Inc. - Allied Reliability Group
J. Federlein	Federlein & Assoc. LLC
B. Fitzpatrick	Wood PLC
J.-P. Hauet	Hauet.com
D. Lee	Avid Solutions Inc.
G. Lehmann	AECOM
T. McAviney	Consultant
V. Mezzano	Fluor Corp.
C. Monchinski	Automated Control Concepts Inc.
G. Nasby	City of Guelph Water Services
M. Nixon	Emerson Process Management
D. Reed	Rockwell Automation
N. Sands	DuPont Company

H. Sasajima
H. Storey
K. Unger
I. Verhappen
D. Visnich
I. Weber
W. Weidman
J. Weiss
D. Zetterberg

Fieldcomm Group Inc. Asia-Pacific
Herman Storey Consulting
Advanced Operational Excellence Co.
Industrial Automation Networks
Burns & McDonnell
Siemens AG DF FA
Consultant
Applied Control Solutions LLC
Chevron Energy Technology Co.

CONTENTS

0	Introduction	13
0.1	Overview	13
0.2	Purpose and intended audience	13
1	Scope	17
2	Normative references	17
3	Terms, definitions, abbreviated terms, acronyms, and conventions	17
3.1	Terms and definitions	17
3.2	Abbreviated terms and acronyms	23
3.3	Conventions	25
4	Common Component Security Constraints	26
4.1	Overview	26
4.2	CCSC 1 Support of essential functions	26
4.3	CCSC 2 Compensating countermeasures	26
4.4	CCSC 3 Least privilege	27
4.5	CCSC 4 Software development process	27
5	FR 1 – Identification and authentication control	27
5.1	Purpose and SL-C(IAC) descriptions	27
5.2	Rationale	27
5.3	CR 1.1 – Human user identification and authentication	27
5.4	CR 1.2 – Software process and device identification and authentication	28
5.5	CR 1.3 – Account management	29
5.6	CR 1.4 – Identifier management	30
5.7	CR 1.5 – Authenticator management	30
5.8	CR 1.6 – Wireless access management	32
5.9	CR 1.7 – Strength of password-based authentication	32
5.10	CR 1.8 – Public key infrastructure certificates	33
5.11	CR 1.9 – Strength of public key-based authentication	33
5.12	CR 1.10 – Authenticator feedback	34
5.13	CR 1.11 – Unsuccessful login attempts	35
5.14	CR 1.12 – System use notification	36
5.15	CR 1.13 – Access via untrusted networks	36
5.16	CR 1.14 – Strength of symmetric key-based authentication	36
6	FR 2 – Use control	37
6.1	Purpose and SL-C(UC) descriptions	37
6.2	Rationale	38
6.3	CR 2.1 – Authorization enforcement	38
6.4	CR 2.2 – Wireless use control	39
6.5	CR 2.3 – Use control for portable and mobile devices	40
6.6	CR 2.4 – Mobile code	40
6.7	CR 2.5 – Session lock	40
6.8	CR 2.6 – Remote session termination	40
6.9	CR 2.7 – Concurrent session control	41

6.10	CR 2.8 – Auditable events.....	41
6.11	CR 2.9 – Audit storage capacity	42
6.12	CR 2.10 – Response to audit processing failures	43
6.13	CR 2.11 – Timestamps.....	43
6.14	CR 2.12 – Non-repudiation.....	44
6.15	CR 2.13 – Use of physical diagnostic and test interfaces	45
7	FR 3 – System integrity	45
7.1	Purpose and SL-C(SI) descriptions	45
7.2	Rationale	45
7.3	CR 3.1 – Communication integrity	45
7.4	CR 3.2 – Protection from malicious code.....	46
7.5	CR 3.3 – Security functionality verification	46
7.6	CR 3.4 – Software and information integrity	47
7.7	CR 3.5 – Input validation.....	48
7.8	CR 3.6 – Deterministic output	48
7.9	CR 3.7 – Error handling	49
7.10	CR 3.8 – Session integrity.....	50
7.11	CR 3.9 – Protection of audit information.....	50
7.12	CR 3.10 – Support for updates.....	51
7.13	CR 3.11 – Physical tamper resistance and detection	51
7.14	CR 3.12 – Provisioning product supplier roots of trust	51
7.15	CR 3.13 – Provisioning asset owner roots of trust	51
7.16	CR 3.14 – Integrity of the boot process	51
8	FR 4 – Data confidentiality	51
8.1	Purpose and SL-C(DC) descriptions.....	51
8.2	Rationale	52
8.3	CR 4.1 – Information confidentiality	52
8.4	CR 4.2 – Information persistence	52
8.5	CR 4.3 – Use of cryptography	53
9	FR 5 – Restricted data flow	54
9.1	Purpose and SL-C(RDF) descriptions.....	54
9.2	Rationale	54
9.3	CR 5.1 – Network segmentation.....	54
9.4	CR 5.2 – Zone boundary protection.....	55
9.5	CR 5.3 – General-purpose person-to-person communication restrictions.....	55
9.6	CR 5.4 – Application partitioning	55
10	FR 6 – Timely response to events	55
10.1	Purpose and SL-C(TRE) descriptions.....	55
10.2	Rationale	56
10.3	CR 6.1 – Audit log accessibility	56
10.4	CR 6.2 – Continuous monitoring.....	56
11	FR 7 – Resource availability.....	57
11.1	Purpose and SL-C(RA) descriptions.....	57
11.2	Rationale	57

11.3	CR 7.1 – Denial of service protection	58
11.4	CR 7.2 – Resource management.....	58
11.5	CR 7.3 – Control system backup	59
11.6	CR 7.4 – Control system recovery and reconstitution	59
11.7	CR 7.5 - Emergency Power	60
11.8	CR 7.6 – Network and security configuration settings.....	60
11.9	CR 7.7 – Least functionality	60
11.10	CR 7.8 – Control system component inventory	61
12	Software application requirements	61
12.1	Purpose	61
12.2	SAR 2.4 – Mobile code.....	61
12.3	SAR 3.2 – Protection from malicious code.....	62
13	Embedded device requirements	63
13.1	Purpose	63
13.2	EDR 2.4 – Mobile code	63
13.3	EDR 2.13 – Use of physical diagnostic and test interfaces	63
13.4	EDR 3.2 – Protection from malicious code	64
13.5	EDR 3.10 – Support for updates.....	65
13.6	EDR 3.11 – Physical tamper resistance and detection.....	65
13.7	EDR 3.12 – Provisioning product supplier roots of trust.....	66
13.8	EDR 3.13 – Provisioning asset owner roots of trust.....	67
13.9	EDR 3.14 – Integrity of the boot process	68
14	Host device requirements.....	68
14.1	Purpose	68
14.2	HDR 2.4 – Mobile code	68
14.3	HDR 2.13 – Use of physical diagnostic and test interfaces	69
14.4	HDR 3.2 – Protection from malicious code	70
14.5	HDR 3.10 – Support for updates	70
14.6	HDR 3.11 – Physical tamper resistance and detection	71
14.7	HDR 3.12 – Provisioning product supplier roots of trust	71
14.8	HDR 3.13 – Provisioning asset owner roots of trust.....	72
14.9	HDR 3.14 – Integrity of the boot process.....	73
15	Network device requirements	73
15.1	Purpose	73
15.2	NDR 1.6 – Wireless access management.....	74
15.3	NDR 1.13 – Access via untrusted networks	74
15.4	NDR 2.4 – Mobile code	75
15.5	NDR 2.13 – Use of physical diagnostic and test interfaces	76
15.6	NDR 3.2 – Protection from malicious code	76
15.7	NDR 3.10 – Support for updates	77
15.8	NDR 3.11 – Physical tamper resistance and detection	77
15.9	NDR 3.12 – Provisioning product supplier roots of trust	78
15.10	NDR 3.13 – Provisioning asset owner roots of trust.....	79
15.11	NDR 3.14 – Integrity of the boot process.....	80

15.12 NDR 5.2 – Zone boundary protection	80
15.13 NDR 5.3 – General purpose, person-to-person communication restrictions	81
Annex A (informative) Device categories	83
A.1 Device categories	83
A.1.1 Device category: embedded device	83
A.1.2 Device category: network device	84
A.1.3 Device category: host device/application	84
Annex B (informative) Mapping of CRs and REs to FR SLs 1-4	87
B.1 Overview.....	87
B.2 SL mapping table	87
Figure 1 – ISA-62443 Work Products	15

FOREWORD

This document is part of a multipart standard that addresses the issue of security for the components which are contained in industrial automation and control systems (IACS). It has been developed by working group 04, task group 4 of the ISA99 committee in cooperation with IEC TC65/WG10.

This document prescribes the security requirements for the components that are used to build control systems. These security requirements are derived from the system requirements for IACS defined in ISA-62443-3-3:2013 [1]¹ and as such, assigns component security levels (SLs) which are based on the system security levels.

¹ Numbers in brackets indicate references in the Bibliography.