Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Setting the Standard for Automation™

AMERICAN NATIONAL STANDARD

ANSI/ISA-62443-4-1-2018

Security for industrial automation and control systems Part 4-1: Product security development life-cycle requirements

Approved 16 February 2018

ANSI/ISA-62443-4-1-2018

Security for industrial automation and control systems

Part 4-1: Product security development life-cycle requirements

ISBN: 978-1-945541-82-7

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-62443-4-1-2018.

This document has been prepared as part of the service of ISA, the International Society for 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 & 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 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.

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 non-profit 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 06 in the preparation of this document:

Name	Company	Contributor	Reviewer
Johan Nye, WG Chair	Exxon		X
Kevin Staggs, WG Chair	Honeywell		X
Michael Medoff, TG Lead	Exida	X	X
Mike Ahmadi	Codenomicon, Ltd.	X	X
Shameem Akhter	Intel Corporation	X	X
Andreas Backman	ABB	X	X
Satish Balasubramanian	Yokogawa IA Technologies	X	X
Eric Braun	Emerson Process Management	X	X
Fabio Buhrer	ABB		X
Eric Cosman	OIT Concepts LLC		X
Ed Crawford	Chevron		X
John Cusimano	AE Solutions	X	X
Emmanuel DelaHostria	Consultant		X
John Feikis	Dell		X
Paul Forney	Schneider Electric	X	X
Ken Frische	AE Solutions		X
Dennis Holstein	OPUS Consulting Group		X
Charles Hoover	SmartWorks		X
Dave Johnson	Exida	X	X
Pierre Kobes	Siemens		X
John Lellis	Berkana Resources Corporation		X
Mike Lester	Emerson Process Management		X
Suzanne Lightman	NIST		X
Roberto Minicucci	GE Oil & Gas	X	X
Rob Mixer	Emerson Process Management	X	X
Lee Neitzel	GE	X	X
Alex Nicoll	Rockwell Automation	X	X
Milind Patwardhan	Schneider Electric		X
Jeff Potter	Emerson Process Management		X
Dan Scali	Mandiant	X	X
Ragnar Schierholz	ABB		X
Byron Schneidau	BP		X
Maik Seewald	Cisco Systems	X	X
Graham Speake	Berkana Resources		X
Tatsuaki Takebe	KPMG Consulting Co., Inc.		X
Bill Thomson	Cisco Systems	X	X
Frank van den Berg	Green Hills Software		X
Gerd Wartman	WSC-WartmannSecurityConsulting		X
Karl-Heinz Walsdorf	Siemens	X	X
Kevin Yoo	GE	X	X

This document was approved for publication by the ISA Standards and Practices Board on 23 January 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	Consultant
J. Federlein	Federlein & Assoc. LLC
B. Fitzpatrick	Wood PLC
J.-P. Hauet	Hauet.com
D. Lee	Avid Solutions Inc.
G. Lehmann	AECOM
K. Lindner	Endress+Hauser Process Solutions AG
T. McAvinew	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	Fieldcomm Group Inc. Asia-Pacific
H. Storey	Herman Storey Consulting
K. Unger	Advanced Operational Excellence Co.
I. Verhappen	Industrial Automation Networks
D. Visnich	Burns & McDonnell
I. Weber	Siemens AG
W. Weidman	Consultant
J. Weiss	Applied Control Solutions LLC
D. Zetterberg	Chevron Energy Technology Co.

CONTENTS

This page intentionally left blank.

Foreword

This document is part of a multipart standard that addresses the issue of security for industrial automation and control systems (IACS). It has been developed by working group 04, task group 06 of the ISA99 committee in cooperation with IEC TC65/WG10.

This document prescribes the activities required to perform security risk assessments on a new or existing IACS and the design activities required to mitigate the risk to tolerable levels.

Prior to reading this document the reader should, at a minimum, be familiar with the basic IACS concepts and terminology which can be found in ANSI/ISA-62443-1-1 (99.01.01) (originally published as an ISA standard ANSI/ISA-99.00.01-2007).

This page intentionally left blank.

Introduction

This document is part of a series of standards that addresses the issue of security for industrial automation and control systems (IACS). This document describes product development life-cycle requirements related to cyber security for products intended for use in the industrial automation and control systems environment and provides guidance on how to meet the requirements described for each element.

This document has been developed in large part from the Secure Development Life-cycle Assessment (SDLA) Certification Requirements [24] from the ISA Security Compliance Institute (ISCI). Note that the SDLA procedure was based on the following sources:

– ISO/IEC 15408-3 (Common Criteria) [16];

– Open Web Application Security Project (OWASP) Comprehensive, Lightweight Application Security Process (CLASP) [35];

– The Security Development Life-cycle by Michael Howard and Steve Lipner [45];

– IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems [22], and

– RCTA DO-178B Software Considerations in Airborne Systems and Equipment Certification [27].

Therefore, all these sources can be considered contributing sources to this standard.

This document is the part of the ISA-62443 series that contains security requirements for developers of any automation and control products where security is a concern.

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 in the list of normative references in Clause 2, and those that are referenced for informational purposes or that are in development are listed in the Bibliography.

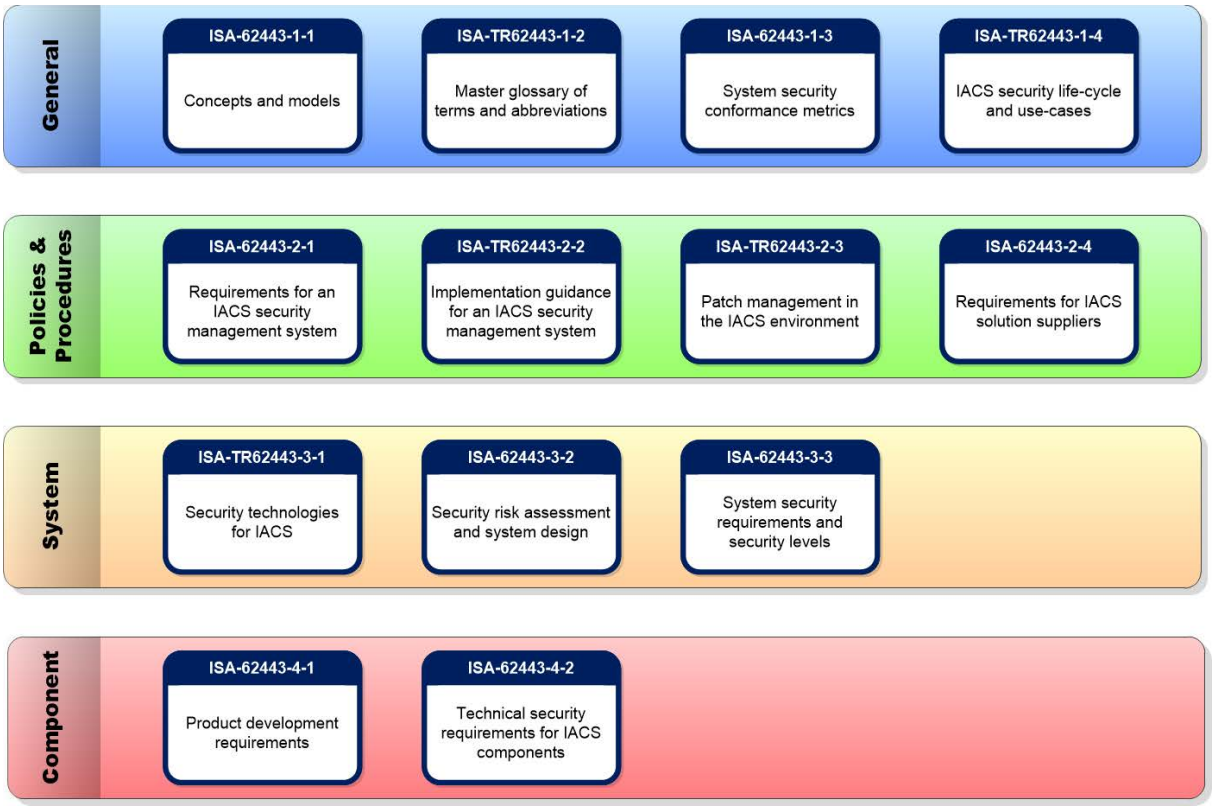

Figure 1 – Parts of the ISA-62443 series

Figure 2 – Example scope of product life-cycle illustrates how the developed product relates to maintenance and integration capabilities defined in IEC 62443-2-4 [5] and to its operation by the asset owner. The product supplier develops products using a process compliant with this standard. Those products may be a single component, such as an embedded controller, or a group of components working together as a system or subsystem. The products are then integrated together, usually by a system integrator, into an Automation Solution using a process compliant with IEC 62443-2-4. The Automation Solution is then installed at a particular site and becomes part of the industrial automation and control system (IACS). Some of these capabilities reference security measures defined in ANSI/ISA-62443-3-3 (99.03.03) [8] that the service provider ensures are supported in the Automation Solution (either as product features or compensating mechanisms). This standard only addresses the process used for the development of the product; it does not address design, installation or operation of the Automation Solution or IACS.

In Figure 2, the Automation Solution is illustrated to contain one or more subsystems and optional supporting components such as advanced control. The dashed boxes indicate that these components are “optional”.

NOTE 1 Automation Solutions typically have a single product, but they are not restricted to do so. In some industries, there may be a hierarchical product structure. In general, the Automation Solution is the set of hardware and software, independent of product packaging, that is used to control a physical process (for example, continuous or manufacturing) as defined by the asset owner.

NOTE 2 If a service provider provides products used in the Automation Solution, then the service provider is fulfilling the role of product supplier in this diagram.

NOTE 3 If a service provider provides products used in the Automation Solution, then the service provider is fulfilling the role of product supplier in this diagram.

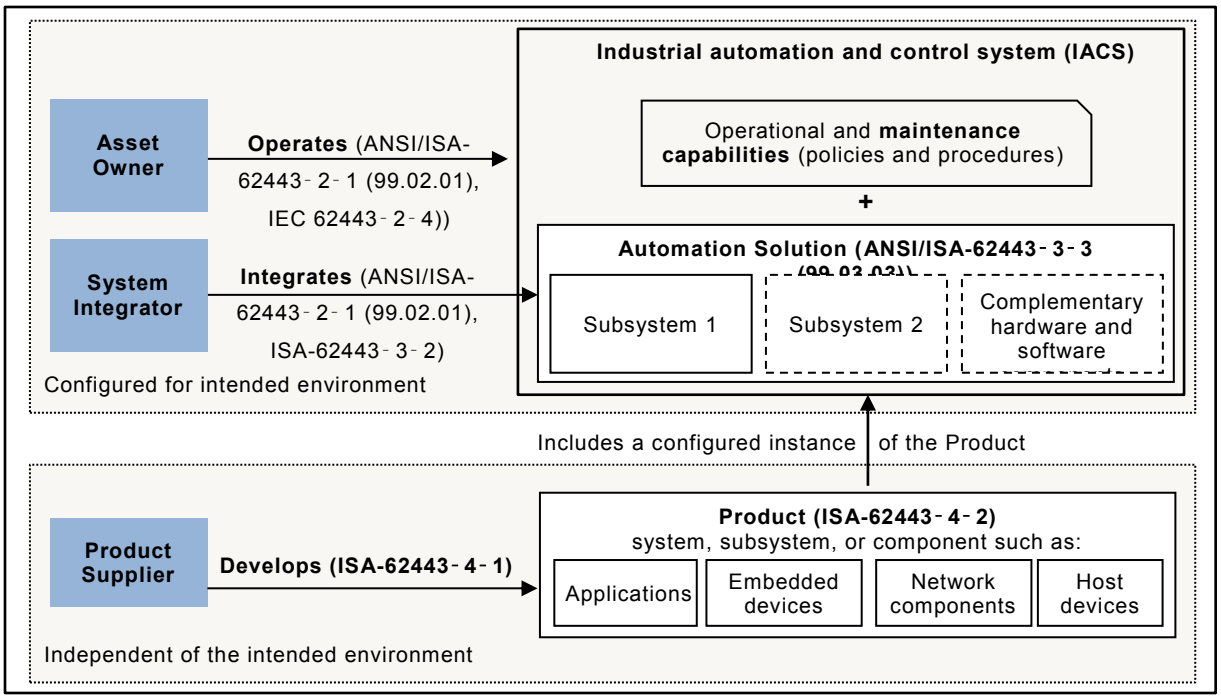

Figure 2 – Example scope of product life-cycle

This page intentionally left blank.

1 Scope

This part of ISA-62443 specifies process requirements for the secure development of products used in industrial automation and control systems. It defines a secure development life-cycle (SDL) for the purpose of developing and maintaining secure products. This life-cycle includes security requirements definition, secure design, secure implementation (including coding guidelines), verification and validation, defect management, patch management and product end-of-life. These requirements can be applied to new or existing processes for developing, maintaining and retiring hardware, software or firmware for new or existing products. These requirements apply to the developer and maintainer of the product, but not to the integrator or user of the product. A summary list of the requirements in this standard can be found in Annex B.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 62443-2-4, *Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers [5]*

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-TR62443-1-2 and the following apply.

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

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

3.1.1
abuse case
test case used to perform negative operations of a use case

Note 1 to entry: Abuse case tests are simulated attacks often based on the threat model. An abuse case is a type of complete interaction between a system and one or more actors where the results of the interaction are intentionally intended to be harmful to the system, one of the actors or one of the stakeholders in the system.

3.1.2
access control <protection>
protection of system resources against unauthorized access

3.1.3
access control <process>
process by which use of system resources is regulated according to a security policy and is permitted by only authorized users according to that policy

Note 1 to entry: Access control includes identification and authentication requirements specified in other parts of the ISA-62443 series.

3.1.4
administrator
users who have been authorized to manage security policies/capabilities for a product or system