Singapore
Standards
Council

SS IEC 62443-4-1 : 2018
IEC 62443-4-1:2018, IDT
(ICS 25.040.40; 35.030)

SINGAPORE STANDARD

Security for industrial automation and control systems –

Part 4-1 : Secure product development lifecycle requirements

Published by

Enterprise
Singapore

SS IEC 62443-4-1 : 2018
IEC 62443-4-1:2018, IDT
(ICS 25.040.40; 35.030)

SINGAPORE STANDARD

Security for industrial automation and control systems –

Part 4-1 : Secure product development lifecycle requirements

ISBN 978-981-48-3539-8

This Singapore Standard was approved on 15 November 2018 by the Manufacturing Standards Committee under the purview of the Singapore Standards Council.

First published, 2019.

The Manufacturing Standards Committee, appointed by the Standards Council, consists of the following members:

		Name	Capacity
Chairman	:	Dr John Yong	*Individual Capacity*
Deputy Chairman	:	Mr Brandon Lee	*Individual Capacity*
Secretary	:	Mr Lee Weiguo	*Singapore Manufacturing Federation – Standards Development Organisation*
Members	:	Ms Fong Pin Fen	*Singapore Economic Development Board*
		Mr Goh Wee Hong	*TÜV SÜD PSB Pte Ltd*
		Mr Ho Chi Bao	*Enterprise Singapore*
		Mr Steven Koh	*Singapore Precision Engineering and Technology Association*
		Ms Lee Wan Sie	*Info-comm Media Development Authority*
		Dr Jim Li Hui Hong	*Individual Capacity*
		Dr Lim Ee Meng	*National Metrology Centre*
		Mr Loh Wai Mun	*Science and Engineering Research Council*
		Er. Prof Seeram Ramakrishan	*The Institution of Engineers, Singapore*

The Technical Committee on Smart Manufacturing, appointed by the Manufacturing Standards Committee, consists of representatives from the following organisations:

		Name	Organisation
Co-Chairmen	:	Mr Yeoh Pit Wee	*Individual Capacity*
		Dr Tan Puay Siew	*Individual Capacity*
Secretary	:	Mr Louis Lauw	*Singapore Manufacturing Federation – Standards Development Organisation*
Members	:	Dr Ian Chan Hian Leng	*Singapore Institute of Manufacturing Technology*
		Mr Cheong Siah Chong	*Singapore Industrial Automation Association*
		Mr David Chia	*Beckhoff Automation Pte Ltd (Southeast Asia)*
		Dr Andreas Hauser	*TÜV SÜD Asia Pacific Pte Ltd*
		Mr Phil Kay	*SP Manufacturing Pte Ltd*
		Mr Sunny Khoo	*Toshiba Tec Singapore Pte Ltd*
		Dr Lai Weng Hong	*Singapore Semiconductor Industry Association*
		Mr Brandon Lee	*Singapore Manufacturing Federation*
		Mr Francis Lee	*TRUMPF Pte Ltd*

		Name	Organisation
Members	:	Prof Lee Loo Hay	*National University of Singapore*
		Mr Zach Lee	*Siemens*
		Mr Gerry Ong	*SMT Technology Pte Ltd*
		Prof John Pang	*Nanyang Technological University*
		Er. Prof Seeram Ramakrishan	*The Institution of Engineers, Singapore*
		Mr Sim Bak Chor	*Infocomm Media Development Authority*
		Mr Brian Teo	*PBA Systems Pte Ltd*
		Mr Stuart Wong	*Advanced Remanufacturing and Technology Centre*

The Working Group on Cyber Security for Industrial Automation, appointed by the Technical Committee on Smart Manufacturing to assist in the preparation of this standard, comprises the following experts who contribute in their *individual capacity*:

		Name
Co-Convenors	:	Dr Andreas Hauser
		Mr Lim Thian Chin
Secretary	:	Mr Louis Lauw
Members	:	Mr Willie Lui Tien Heong
		Mr Thomas Quek
		Mr Sherkar Suhas Laxman
		Mr Henry Tan
		Mr William Temple
		Dr Vrizlynn Thing
		Mr Vishram Mishra
		Mr Timothy Yong
		Mr Bobby Zhou WenBo

The organisations in which experts of the Working Group are involved are:

Advanced Digital Sciences Center
Cyber Security Agency of Singapore
Huawei International Pte Ltd
Infineon Technologies Asia Pacific Pte Ltd
Institute for Infocomm Research
MicroSec Pte Ltd
REDCON Security Advisors LLP
Temasek Polytechnic
TÜV SÜD Asia Pacific Pte Ltd

(blank page)

CONTENTS

NATIONAL FOREWORD 10
FOREWORD 11
INTRODUCTION 13
1 Scope 16
2 Normative references 16
3 Terms, definitions, abbreviated terms, acronyms and conventions 16
3.1 Terms and definitions 16
3.2 Abbreviated terms and acronyms 22
3.3 Conventions 22
4 General principles 23
4.1 Concepts 23
4.2 Maturity model 24
5 Practice 1 – Security management 26
5.1 Purpose 26
5.2 SM-1: Development process 27
5.2.1 Requirement 27
5.3 Rationale and supplemental guidance 27
5.4 SM-2: Identification of responsibilities 27
5.4.1 Requirement 27
5.4.2 Rationale and supplemental guidance 27
5.5 SM-3: Identification of applicability 27
5.5.1 Requirement 27
5.5.2 Rationale and supplemental guidance 28
5.6 SM-4: Security expertise 28
5.6.1 Requirement 28
5.6.2 Rationale and supplemental guidance 28
5.7 SM-5: Process scoping 28
5.7.1 Requirement 28
5.7.2 Rationale and supplemental guidance 29
5.8 SM-6: File integrity 29
5.8.1 Requirement 29
5.8.2 Rationale and supplemental guidance 29
5.9 SM-7: Development environment security 29
5.9.1 Requirement 29
5.9.2 Rationale and supplemental guidance 29
5.10 SM-8: Controls for private keys 30
5.10.1 Requirement 30
5.10.2 Rationale and supplemental guidance 30
5.11 SM-9: Security requirements for externally provided components 30
5.11.1 Requirement 30
5.11.2 Rationale and supplemental guidance 30
5.12 SM-10: Custom developed components from third-party suppliers 31

5.12.1 Requirement 31
5.12.2 Rationale and supplemental guidance 31
5.13 SM-11: Assessing and addressing security-related issues 31
5.13.1 Requirement 31
5.13.2 Rationale and supplemental guidance 31
5.14 SM-12: Process verification 31
5.14.1 Requirement 31
5.14.2 Rationale and supplemental guidance 31
5.15 SM-13: Continuous improvement 32
5.15.1 Requirement 32
5.15.2 Rationale and supplemental guidance 32
6 Practice 2 – Specification of security requirements 33
6.1 Purpose 33
6.2 SR-1: Product security context 33
6.2.1 Requirement 33
6.2.2 Rationale and supplemental guidance 33
6.3 SR-2: Threat model 33
6.3.1 Requirement 33
6.3.2 Rationale and supplemental guidance 34
6.4 SR-3: Product security requirements 35
6.4.1 Requirement 35
6.4.2 Rationale and supplemental guidance 35
6.5 SR-4: Product security requirements content 35
6.5.1 Requirement 35
6.5.2 Rationale and supplemental guidance 35
6.6 SR-5: Security requirements review 35
6.6.1 Requirement 35
6.6.2 Rationale and supplemental guidance 36
7 Practice 3 – Secure by design 36
7.1 Purpose 36
7.2 SD-1: Secure design principles 36
7.2.1 Requirement 36
7.2.2 Rationale and supplemental guidance 37
7.3 SD-2: Defense in depth design 38
7.3.1 Requirement 38
7.3.2 Rationale and supplemental guidance 38
7.4 SD-3: Security design review 38
7.4.1 Requirement 38
7.4.2 Rationale and supplemental guidance 38
7.5 SD-4: Secure design best practices 39
7.5.1 Requirement 39
7.5.2 Rationale and supplemental guidance 39
8 Practice 4 – Secure implementation 39
8.1 Purpose 39
8.2 Applicability 40

8.3 SI-1: Security implementation review 40
8.3.1 Requirement 40
8.3.2 Rationale and supplemental guidance 40
8.4 SI-2: Secure coding standards 40
8.4.1 Requirement 40
8.4.2 Rationale and supplemental guidance 41
9 Practice 5 – Security verification and validation testing 41
9.1 Purpose 41
9.2 SVV-1: Security requirements testing 41
9.2.1 Requirement 41
9.2.2 Rationale and supplemental guidance 41
9.3 SVV-2: Threat mitigation testing 42
9.3.1 Requirement 42
9.3.2 Rationale and supplemental guidance 42
9.4 SVV-3: Vulnerability testing 42
9.4.1 Requirement 42
9.4.2 Rationale and supplemental guidance 43
9.5 SVV-4: Penetration testing 43
9.5.1 Requirement 43
9.5.2 Rationale and supplemental guidance 43
9.6 SVV-5: Independence of testers 43
9.6.1 Requirement 43
9.6.2 Rationale and supplemental guidance 44
10 Practice 6 – Management of security-related issues 44
10.1 Purpose 44
10.2 DM-1: Receiving notifications of security-related issues 45
10.2.1 Requirement 45
10.2.2 Rationale and supplemental guidance 45
10.3 DM-2: Reviewing security-related issues 45
10.3.1 Requirement 45
10.3.2 Rationale and supplemental guidance 46
10.4 DM-3: Assessing security-related issues 46
10.4.1 Requirement 46
10.4.2 Rationale and supplemental guidance 46
10.5 DM-4: Addressing security-related issues 47
10.5.1 Requirement 47
10.5.2 Rationale and supplemental guidance 47
10.6 DM-5: Disclosing security-related issues 48
10.6.1 Requirement 48
10.6.2 Rationale and supplemental guidance 48
10.7 DM-6: Periodic review of security defect management practice 49
10.7.1 Requirement 49
10.7.2 Rationale and supplemental guidance 49
11 Practice 7 – Security update management 49
11.1 Purpose 49

11.2 SUM-1: Security update qualification ... 49
11.2.1 Requirement ... 49
11.2.2 Rationale and supplemental guidance ... 49
11.3 SUM-2: Security update documentation ... 50
11.3.1 Requirement ... 50
11.3.2 Rationale and supplemental guidance ... 50
11.4 SUM-3: Dependent component or operating system security update documentation ... 50
11.4.1 Requirement ... 50
11.4.2 Rationale and supplemental guidance ... 50
11.5 SUM-4: Security update delivery ... 50
11.5.1 Requirement ... 50
11.5.2 Rationale and supplemental guidance ... 51
11.6 SUM-5: Timely delivery of security patches ... 51
11.6.1 Requirement ... 51
11.6.2 Rationale and supplemental guidance ... 51
12 Practice 8 – Security guidelines ... 51
12.1 Purpose ... 51
12.2 SG-1: Product defense in depth ... 52
12.2.1 Requirement ... 52
12.2.2 Rationale and supplemental guidance ... 52
12.3 SG-2: Defense in depth measures expected in the environment ... 52
12.3.1 Requirement ... 52
12.3.2 Rationale and supplemental guidance ... 52
12.4 SG-3: Security hardening guidelines ... 53
12.4.1 Requirement ... 53
12.4.2 Rationale and supplemental guidance ... 53
12.5 SG-4: Secure disposal guidelines ... 53
12.5.1 Requirement ... 53
12.5.2 Rationale and supplemental guidance ... 54
12.6 SG-5: Secure operation guidelines ... 54
12.6.1 Requirement ... 54
12.6.2 Rationale and supplemental guidance ... 54
12.7 SG-6: Account management guidelines ... 54
12.7.1 Requirement ... 54
12.7.2 Rationale and supplemental guidance ... 54
12.8 SG-7: Documentation review ... 55
12.8.1 Requirement ... 55
12.8.2 Rationale and supplemental guidance ... 55
Annex A (informative) Possible metrics ... 56
Annex B (informative) Table of requirements ... 58
Bibliography ... 60

Figure 1 – Parts of the IEC 62443 series ... 14
Figure 2 – Example scope of product life-cycle ... 15

Figure 3 – Defence in depth strategy is a key philosophy of the secure product life-cycle 24

Table 1 – Maturity levels 26
Table 2 – Example SDL continuous improvement activities 32
Table 3 – Required level of independence of testers from developers 44
Table B.1 – Summary of all requirements 58

National Foreword

This Singapore Standard was prepared by the Working Group on Cyber Security for Industrial Automation appointed by the Technical Committee on Smart Manufacturing under the purview of the Manufacturing Standards Committee.

This standard is identical with IEC 62443-4-1:2018, “Security for industrial automation and control systems – Part 4-1 : Secure product development lifecycle requirements”, published by the International Electrotechnical Commission.

Where reference to a particular part of IEC 62443 is made, the appropriate Singapore Standard (which is an identical adoption of that part of IEC 62443) shall apply.

This standard is expected to be used by product suppliers. It can provide references to asset owners and system integrators.

Attention is drawn to the possibility that some of the elements of this Singapore Standard may be the subject of patent rights. Enterprise Singapore shall not be held responsible for identifying any or all of such patent rights.

NOTE

1. *Singapore Standards (SSs) and Technical References (TRs) are reviewed periodically to keep abreast of technical changes, technological developments and industry practices. The changes are documented through the issue of either amendments or revisions.*

2. *An SS or TR is voluntary in nature except when it is made mandatory by a regulatory authority. It can also be cited in contracts making its application a business necessity. Users are advised to assess and determine whether the SS or TR is suitable for their intended use or purpose. If required, they should refer to the relevant professionals or experts for advice on the use of the document. Enterprise Singapore shall not be liable for any damages whether directly or indirectly suffered by anyone or any organisation as a result of the use of any SS or TR.*

3. *Compliance with a SS or TR does not exempt users from any legal obligations.*

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 4-1: Secure product development lifecycle requirements

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62443-4-1 has been prepared by IEC technical committee 65: Industrial-process measurement, control and automation.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
65/685/FDIS	65/688/RVD

Full information on the voting for the approval of this International Standard can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts in the IEC 62443 series, published under the general title *Security for industrial automation and control systems*, can be found on the IEC website.

Future standards in this series will carry the new general title as cited above. Titles of existing standards in this series will be updated at the time of the next edition.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

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 [26] [1] from the ISA Security Compliance Institute (ISCI). Note that the SDLA procedure was based on the following sources:

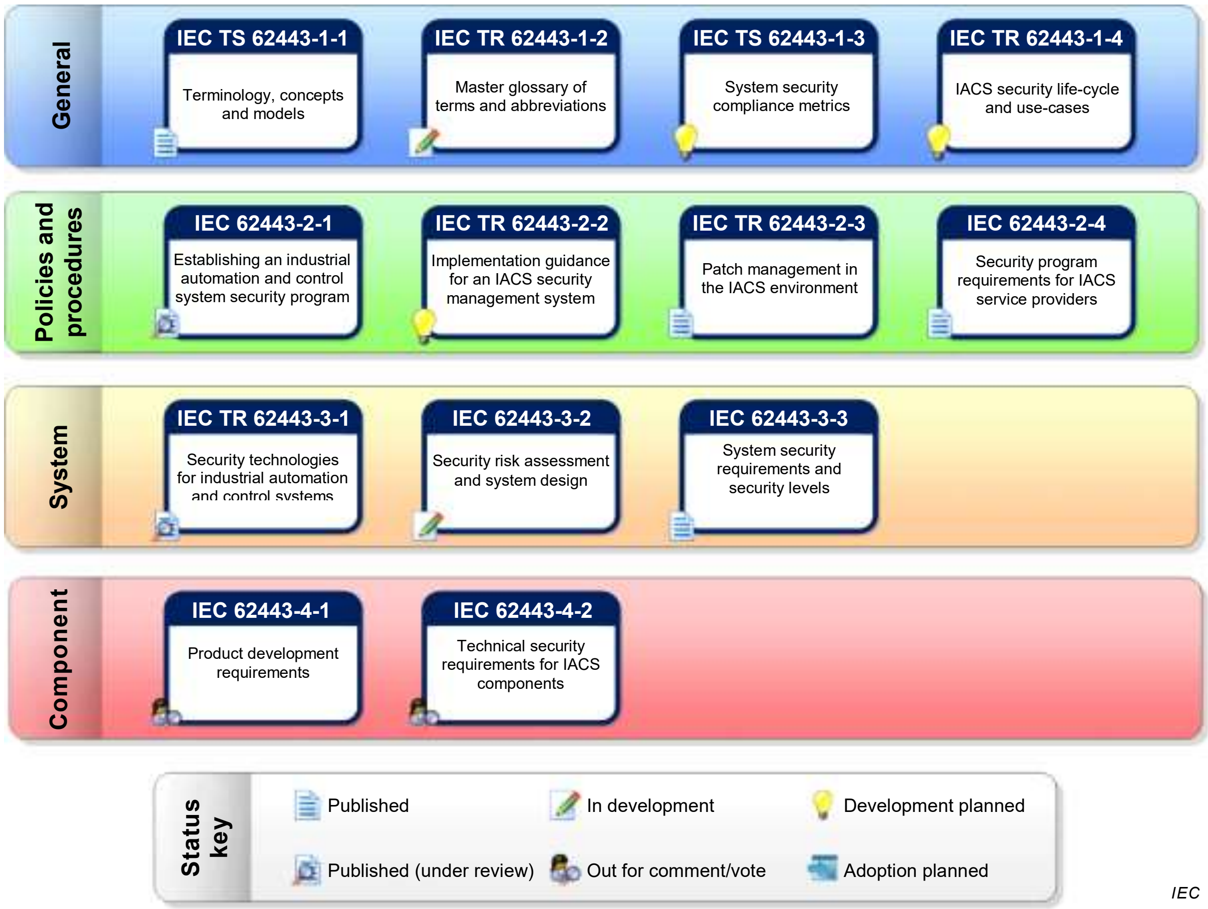
- ISO/IEC 15408-3 (Common Criteria) [18];
- Open Web Application Security Project (OWASP) Comprehensive, Lightweight Application Security Process (CLASP) [36];
- The Security Development Life-cycle by Michael Howard and Steve Lipner [43];
- IEC 61508 Functional safety of electrical/electronic/ programmable electronic safety-related systems [24], and
- RCTA DO-178B Software Considerations in Airborne Systems and Equipment Certification [28].

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

This document is the part of the IEC 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 IEC 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.

[1] Figures in square brackets refer to the bibliography.


General
IEC TS 62443-1-1
Terminology, concepts and models
IEC TR 62443-1-2
Master glossary of terms and abbreviations
IEC TS 62443-1-3
System security compliance metrics
IEC TR 62443-1-4
IACS security life-cycle and use-cases
Policies and procedures
IEC 62443-2-1
Establishing an industrial automation and control system security program
IEC TR 62443-2-2
Implementation guidance for an IACS security management system
IEC TR 62443-2-3
Patch management in the IACS environment
IEC 62443-2-4
Security program requirements for IACS service providers
System
IEC TR 62443-3-1
Security technologies for industrial automation and control systems
IEC 62443-3-2
Security risk assessment and system design
IEC 62443-3-3
System security requirements and security levels
Component
IEC 62443-4-1
Product development requirements
IEC 62443-4-2
Technical security requirements for IACS components
Status key
Published
In development
Development planned
Published (under review)
Out for comment/vote
Adoption planned

IEC

Figure 1 – Parts of the IEC 62443 series

Figure 2 illustrates how the developed product relates to maintenance and integration capabilities defined in IEC 62443-2-4 and to its operation by the asset owner. The product supplier develops products using a process compliant with this document. 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 IEC 62443-3-3 [10] that the service provider ensures are supported in the Automation Solution (either as product features or compensating mechanisms). This document 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.

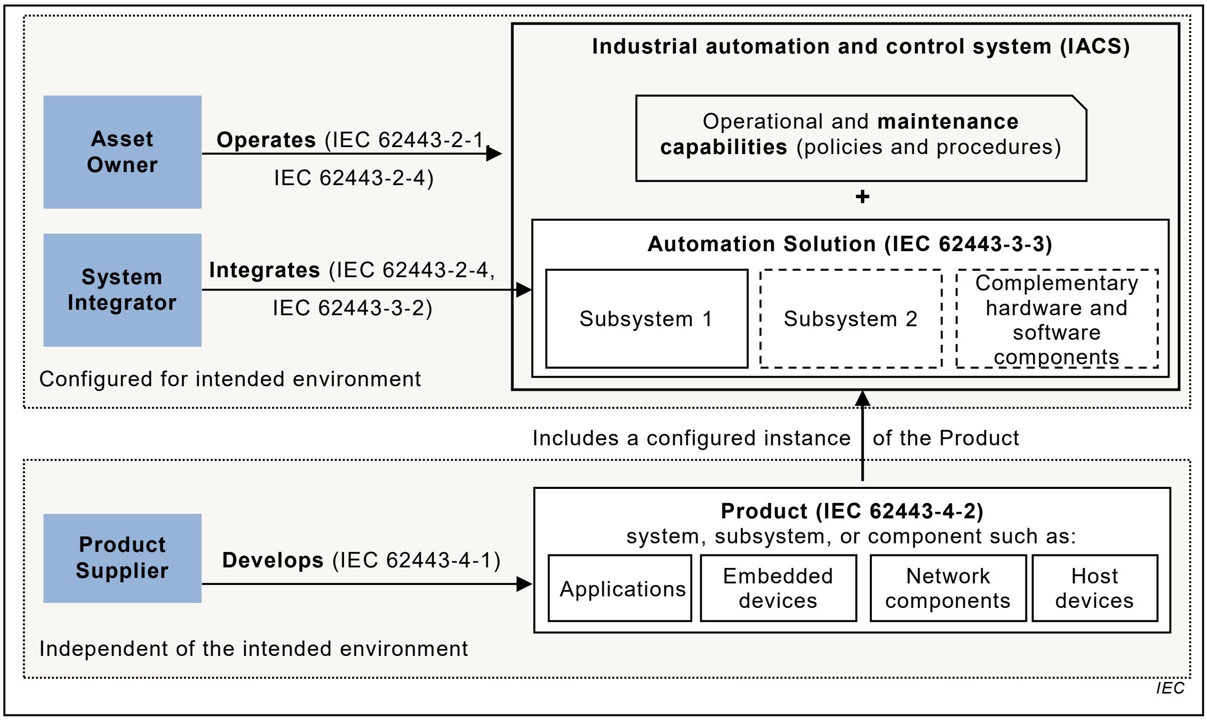

Industrial automation and control system (IACS)
Asset Owner
Operates (IEC 62443-2-1, IEC 62443-2-4)
Operational and maintenance capabilities (policies and procedures)
+
System Integrator
Integrates (IEC 62443-2-4, IEC 62443-3-2)
Automation Solution (IEC 62443-3-3)
Subsystem 1
Subsystem 2
Complementary hardware and software components
Configured for intended environment
Includes a configured instance of the Product
Product Supplier
Develops (IEC 62443-4-1)
Product (IEC 62443-4-2)
system, subsystem, or component such as:
Applications
Embedded devices
Network components
Host devices
Independent of the intended environment
IEC

Figure 2 – Example scope of product life-cycle

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 4-1: Secure product development lifecycle requirements

1 Scope

This part of IEC 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 document 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 62443-2-4:2015, *Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers*
IEC 62443-2-4:2015/AMD1:2017

[2] Under consideration.