

This is a preview of "BS EN IEC 62443-4-1:....". [Click here to purchase the full version from the ANSI store.](#)



BSI Standards Publication

## Security for industrial automation and control systems

---

Part 4-1: Secure product development lifecycle  
requirements (IEC 62443-4-1:2018)

This is a preview of "BS EN IEC 62443-4-1:2018". [Click here to purchase the full version from the ANSI store.](#)

## National foreword

This British Standard is the UK implementation of EN IEC 62443-4-1:2018. It is identical to IEC 62443-4-1:2018.

The UK participation in its preparation was entrusted to Technical Committee GEL/65, Measurement and control.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2018  
Published by BSI Standards Limited 2018

ISBN 978 0 580 89911 9

ICS 25.040.40; 35.030

**Compliance with a British Standard cannot confer immunity from legal obligations.**

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 April 2018.

### Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

---

This is a preview of "BS EN IEC 62443-4-1:....". [Click here to purchase the full version from the ANSI store.](#)

EUROPÄISCHE NORM

March 2018

ICS 25.040.40; 35.030

English Version

Security for industrial automation and control systems - Part 4-1:  
Secure product development lifecycle requirements  
(IEC 62443-4-1:2018)

To be completed  
(IEC 62443-4-1:2018)

IT-Sicherheit für industrielle Automatisierungssysteme - Teil  
4-1: Anforderungen an den Lebenszyklus für eine sichere  
Produktentwicklung  
(IEC 62443-4-1:2018)

This European Standard was approved by CENELEC on 2018-02-19. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



European Committee for Electrotechnical Standardization  
Comité Européen de Normalisation Electrotechnique  
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

This is a preview of "BS EN IEC 62443-4-1:....". [Click here to purchase the full version from the ANSI store.](#)

### **European foreword**

The text of document 65/685/FDIS, future edition 1 of IEC 62443-4-1, prepared by IEC/TC 65 "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 62443-4-1:2018.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2018-11-19
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2021-02-19

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

### **Endorsement notice**

The text of the International Standard IEC 62443-4-1:2018 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 62740	NOTE	Harmonized as EN 62470.
IEC 61508 (series)	NOTE	Harmonized as EN 61508 (series).
ISO/IEC 27001	NOTE	Harmonized as EN ISO/IEC 27001.
ISO/IEC 27002	NOTE	Harmonized as EN ISO/IEC 27002.
ISO 9001	NOTE	Harmonized as EN ISO 9001.

This is a preview of "BS EN IEC 62443-4-1:....". Click here to purchase the full version from the ANSI store.

(normative)

### Normative references to international publications with their corresponding European publications

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.

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: [www.cenelec.eu](http://www.cenelec.eu).

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 62443-2-4	2015	Security for industrial process measurement and control - Network and system security - Part 2-4: Certification of IACS supplier security policies and practices	-	-
+ A1	2017		-	-

This is a preview of "BS EN IEC 62443-4-1:....". [Click here to purchase the full version from the ANSI store.](#)

This is a preview of "BS EN IEC 62443-4-1:....". [Click here to purchase the full version from the ANSI store.](#)

## CONTENTS

FOREWORD.....	6
INTRODUCTION.....	8
1 Scope.....	11
2 Normative references .....	11
3 Terms, definitions, abbreviated terms, acronyms and conventions.....	11
3.1 Terms and definitions.....	11
3.2 Abbreviated terms and acronyms .....	16
3.3 Conventions.....	17
4 General principles .....	17
4.1 Concepts .....	17
4.2 Maturity model .....	19
5 Practice 1 – Security management .....	20
5.1 Purpose .....	20
5.2 SM-1: Development process .....	21
5.2.1 Requirement.....	21
5.3 Rationale and supplemental guidance.....	21
5.4 SM-2: Identification of responsibilities .....	21
5.4.1 Requirement.....	21
5.4.2 Rationale and supplemental guidance.....	21
5.5 SM-3: Identification of applicability.....	21
5.5.1 Requirement.....	21
5.5.2 Rationale and supplemental guidance.....	22
5.6 SM-4: Security expertise .....	22
5.6.1 Requirement.....	22
5.6.2 Rationale and supplemental guidance.....	22
5.7 SM-5: Process scoping .....	22
5.7.1 Requirement.....	22
5.7.2 Rationale and supplemental guidance.....	23
5.8 SM-6: File integrity.....	23
5.8.1 Requirement.....	23
5.8.2 Rationale and supplemental guidance.....	23
5.9 SM-7: Development environment security .....	23
5.9.1 Requirement.....	23
5.9.2 Rationale and supplemental guidance.....	23
5.10 SM-8: Controls for private keys .....	23
5.10.1 Requirement.....	23
5.10.2 Rationale and supplemental guidance.....	24
5.11 SM-9: Security requirements for externally provided components.....	24
5.11.1 Requirement.....	24
5.11.2 Rationale and supplemental guidance.....	24
5.12 SM-10: Custom developed components from third-party suppliers .....	24
5.12.1 Requirement.....	24
5.12.2 Rationale and supplemental guidance.....	25
5.13 SM-11: Assessing and addressing security-related issues .....	25
5.13.1 Requirement.....	25
5.13.2 Rationale and supplemental guidance.....	25

This is a preview of "BS EN IEC 62443-4-1:....". [Click here to purchase the full version from the ANSI store.](#)

5.14	SM-12: Process verification .....	25
5.14.1	Requirement.....	25
5.14.2	Rationale and supplemental guidance.....	25
5.15	SM-13: Continuous improvement .....	25
5.15.1	Requirement.....	25
5.15.2	Rationale and supplemental guidance.....	26
6	Practice 2 – Specification of security requirements .....	26
6.1	Purpose .....	26
6.2	SR-1: Product security context.....	27
6.2.1	Requirement.....	27
6.2.2	Rationale and supplemental guidance.....	27
6.3	SR-2: Threat model.....	27
6.3.1	Requirement.....	27
6.3.2	Rationale and supplemental guidance.....	28
6.4	SR-3: Product security requirements.....	28
6.4.1	Requirement.....	28
6.4.2	Rationale and supplemental guidance.....	28
6.5	SR-4: Product security requirements content .....	29
6.5.1	Requirement.....	29
6.5.2	Rationale and supplemental guidance.....	29
6.6	SR-5: Security requirements review .....	29
6.6.1	Requirement.....	29
6.6.2	Rationale and supplemental guidance.....	29
7	Practice 3 – Secure by design .....	30
7.1	Purpose .....	30
7.2	SD-1: Secure design principles .....	30
7.2.1	Requirement.....	30
7.2.2	Rationale and supplemental guidance.....	30
7.3	SD-2: Defense in depth design.....	31
7.3.1	Requirement.....	31
7.3.2	Rationale and supplemental guidance.....	32
7.4	SD-3: Security design review .....	32
7.4.1	Requirement.....	32
7.4.2	Rationale and supplemental guidance.....	32
7.5	SD-4: Secure design best practices .....	32
7.5.1	Requirement.....	32
7.5.2	Rationale and supplemental guidance.....	33
8	Practice 4 – Secure implementation.....	33
8.1	Purpose .....	33
8.2	Applicability .....	33
8.3	SI-1: Security implementation review .....	33
8.3.1	Requirement.....	33
8.3.2	Rationale and supplemental guidance.....	34
8.4	SI-2: Secure coding standards .....	34
8.4.1	Requirement.....	34
8.4.2	Rationale and supplemental guidance.....	34
9	Practice 5 – Security verification and validation testing.....	34
9.1	Purpose .....	34



This is a preview of "BS EN IEC 62443-4-1:....". [Click here to purchase the full version from the ANSI store.](#)

9.2	SVV-1: Security requirements testing .....	35
9.2.1	Requirement .....	35
9.2.2	Rationale and supplemental guidance .....	35
9.3	SVV-2: Threat mitigation testing .....	35
9.3.1	Requirement .....	35
9.3.2	Rationale and supplemental guidance .....	35
9.4	SVV-3: Vulnerability testing .....	36
9.4.1	Requirement .....	36
9.4.2	Rationale and supplemental guidance .....	36
9.5	SVV-4: Penetration testing .....	36
9.5.1	Requirement .....	36
9.5.2	Rationale and supplemental guidance .....	36
9.6	SVV-5: Independence of testers .....	37
9.6.1	Requirement .....	37
9.6.2	Rationale and supplemental guidance .....	37
10	Practice 6 – Management of security-related issues .....	38
10.1	Purpose .....	38
10.2	DM-1: Receiving notifications of security-related issues .....	38
10.2.1	Requirement .....	38
10.2.2	Rationale and supplemental guidance .....	38
10.3	DM-2: Reviewing security-related issues .....	38
10.3.1	Requirement .....	38
10.3.2	Rationale and supplemental guidance .....	39
10.4	DM-3: Assessing security-related issues .....	39
10.4.1	Requirement .....	39
10.4.2	Rationale and supplemental guidance .....	39
10.5	DM-4: Addressing security-related issues .....	40
10.5.1	Requirement .....	40
10.5.2	Rationale and supplemental guidance .....	40
10.6	DM-5: Disclosing security-related issues .....	41
10.6.1	Requirement .....	41
10.6.2	Rationale and supplemental guidance .....	41
10.7	DM-6: Periodic review of security defect management practice .....	42
10.7.1	Requirement .....	42
10.7.2	Rationale and supplemental guidance .....	42
11	Practice 7 – Security update management .....	42
11.1	Purpose .....	42
11.2	SUM-1: Security update qualification .....	42
11.2.1	Requirement .....	42
11.2.2	Rationale and supplemental guidance .....	42
11.3	SUM-2: Security update documentation .....	42
11.3.1	Requirement .....	42
11.3.2	Rationale and supplemental guidance .....	43
11.4	SUM-3: Dependent component or operating system security update documentation .....	43
11.4.1	Requirement .....	43
11.4.2	Rationale and supplemental guidance .....	43
11.5	SUM-4: Security update delivery .....	43
11.5.1	Requirement .....	43

This is a preview of "BS EN IEC 62443-4-1:2018". [Click here to purchase the full version from the ANSI store.](#)

11.5.2	Rationale and supplemental guidance.....	43
11.6	SUM-5: Timely delivery of security patches.....	44
11.6.1	Requirement.....	44
11.6.2	Rationale and supplemental guidance.....	44
12	Practice 8 – Security guidelines.....	44
12.1	Purpose.....	44
12.2	SG-1: Product defense in depth.....	44
12.2.1	Requirement.....	44
12.2.2	Rationale and supplemental guidance.....	45
12.3	SG-2: Defense in depth measures expected in the environment.....	45
12.3.1	Requirement.....	45
12.3.2	Rationale and supplemental guidance.....	45
12.4	SG-3: Security hardening guidelines.....	45
12.4.1	Requirement.....	45
12.4.2	Rationale and supplemental guidance.....	46
12.5	SG-4: Secure disposal guidelines.....	46
12.5.1	Requirement.....	46
12.5.2	Rationale and supplemental guidance.....	46
12.6	SG-5: Secure operation guidelines.....	46
12.6.1	Requirement.....	46
12.6.2	Rationale and supplemental guidance.....	47
12.7	SG-6: Account management guidelines.....	47
12.7.1	Requirement.....	47
12.7.2	Rationale and supplemental guidance.....	47
12.8	SG-7: Documentation review.....	47
12.8.1	Requirement.....	47
12.8.2	Rationale and supplemental guidance.....	47
Annex A (informative)	Possible metrics.....	48
Annex B (informative)	Table of requirements.....	50
Bibliography	.....	52
Figure 1 – Parts of the IEC 62443 series.....		9
Figure 2 – Example scope of product life-cycle.....		10
Figure 3 – Defence in depth strategy is a key philosophy of the secure product life-cycle.....		18
Table 1 – Maturity levels.....		20
Table 2 – Example SDL continuous improvement activities.....		26
Table 3 – Required level of independence of testers from developers.....		37
Table B.1 – Summary of all requirements.....		50

This is a preview of "BS EN IEC 62443-4-1:....". Click here to purchase the full version from the ANSI store.

## 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.

This is a preview of "BS EN IEC 62443-4-1:....". [Click here to purchase the full version from the ANSI store.](#)

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.**

This is a preview of "BS EN IEC 62443-4-1:....". [Click here to purchase the full version from the ANSI store.](#)

## 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]<sup>1</sup> 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.

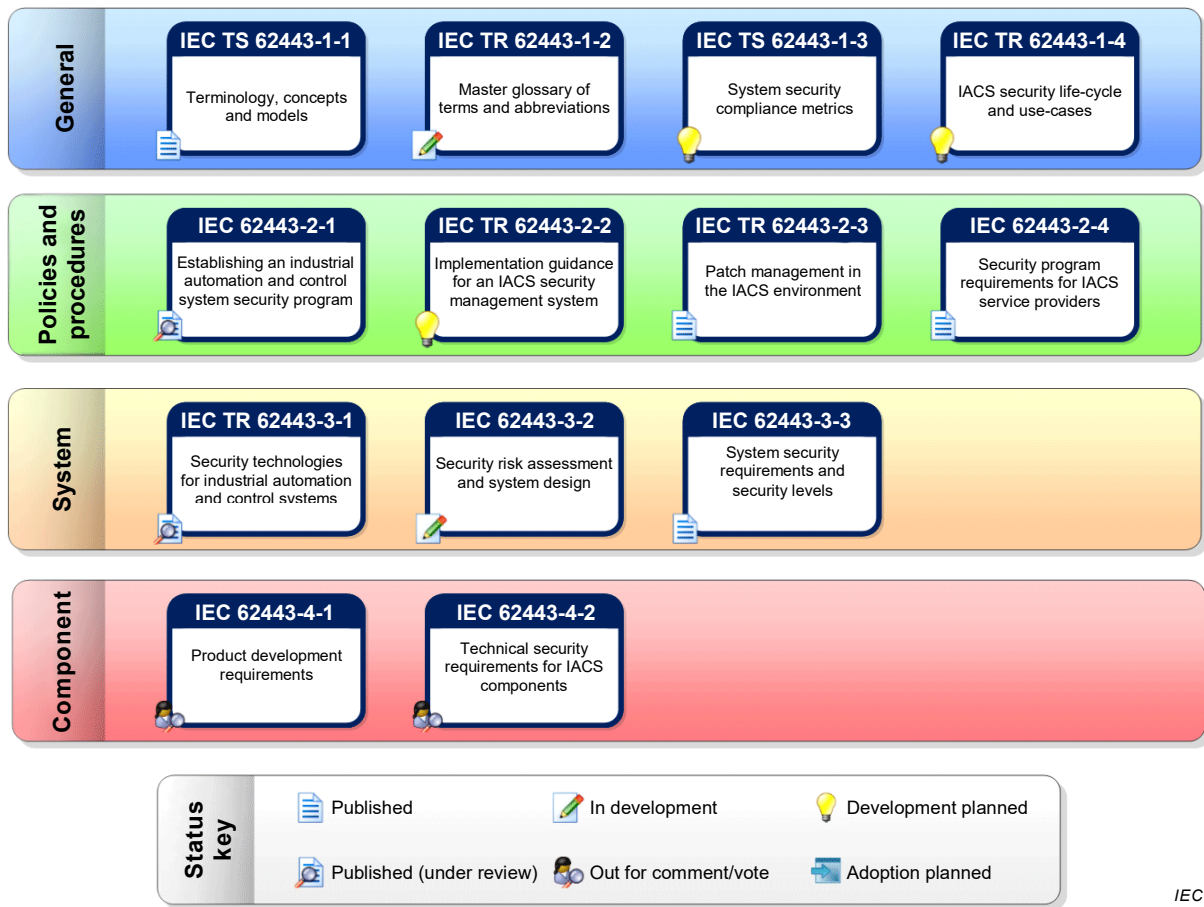
This document is the part of the IEC 62443 series that contains security requirements for developers of any automation and control products where security is a concern.

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.

---

<sup>1</sup> Figures in square brackets refer to the bibliography.

This is a preview of "BS EN IEC 62443-4-1:...". Click here to purchase the full version from the ANSI store.



**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.

This is a preview of "BS EN IEC 62443-4-1:....". Click here to purchase the full version from the ANSI store.

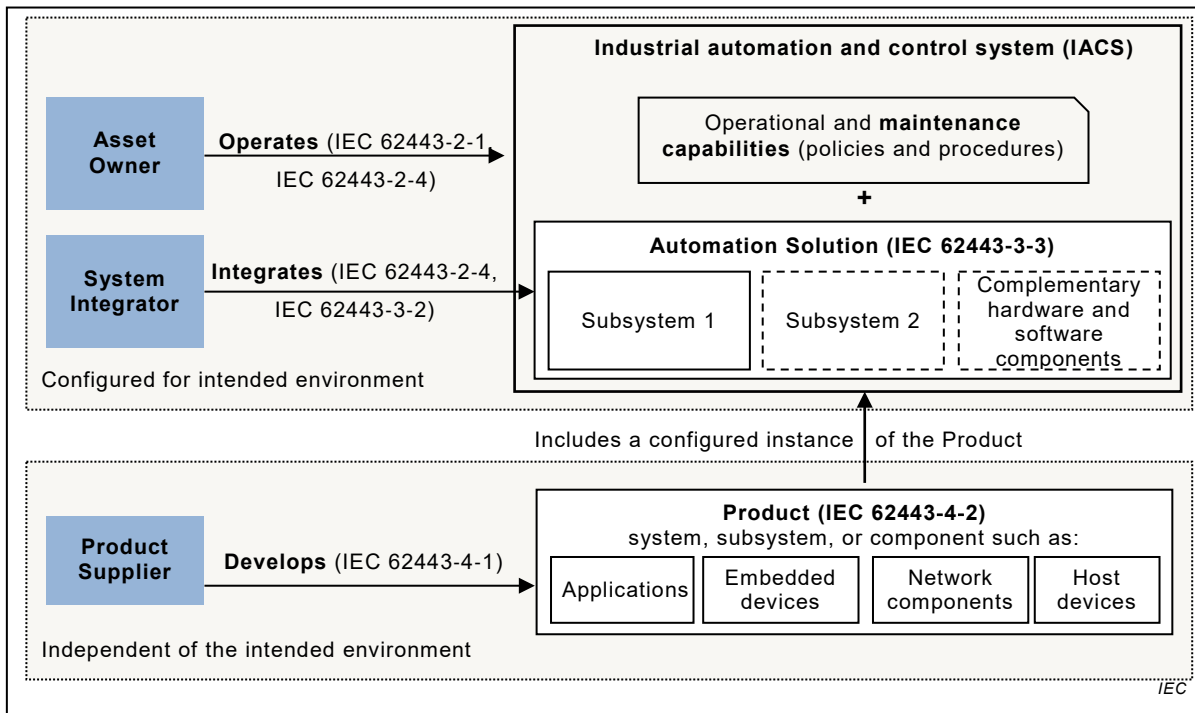


Figure 2 – Example scope of product life-cycle

This is a preview of "BS EN IEC 62443-4-1:....". Click here to purchase the full version from the ANSI store.

## 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

#### 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 IEC TR 62443-1-2<sup>2</sup> 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.

---

<sup>2</sup> Under consideration.