

AS IEC 62443.4.1:2024
IEC 62443-4-1:2018



Security for industrial automation and control systems

Part 4.1: Secure product development lifecycle requirements



AS IEC 62443.4.1:2024

This Australian Standard® was prepared by IT-006, Industrial Process Measurement, Control and Automation. It was approved on behalf of Standards Australia's Standards Development and Accreditation Committee on 22 April 2024.

This Standard was published on 3 May 2024.

The following are represented on Committee IT-006:

- Australia Safety Critical Systems Association
- Australian Computer Society
- Australian Energy Producers
- Australian Industry Group
- Engineers Australia
- ISACA Sydney
- Institute of Instrumentation, Control and Automation Australia
- Workplace Health and Safety Queensland

This Standard was issued in draft form for comment as DR AS IEC 62443.4.1:2024.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:

www.standards.org.au

ISBN 978 1 76139 626 7

Security for industrial automation and control systems

Part 4.1: Secure product development lifecycle requirements

First published as AS IEC 62443.4.1:2024.



Standards Australia Ltd 2024

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968 (Cth).

Preface

This Standard was prepared by the Standards Australia Committee IT-006, Industrial Process Measurement, Control and Automation.

The objective of this document is to specify 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 are intended for the developer and maintainer of the product, but not the integrator or user of the product. A summary list of the requirements in this document can be found in Annex B.

This document is identical with, and has been reproduced from, IEC 62443-4-1:2018, *Industrial communication networks — Network and system security — Part 4-1: Secure product development lifecycle requirements*.

As this document has been reproduced from an International document, a full point substitutes for a comma when referring to a decimal marker.

Australian or Australian/New Zealand Standards that are identical adoptions of international normative references may be used interchangeably. Refer to the online catalogue for information on specific Standards.

The terms “normative” and “informative” are used in Standards to define the application of the appendices or annexes to which they apply. A “normative” appendix or annex is an integral part of a Standard, whereas an “informative” appendix or annex is only for information and guidance.

Contents

Preface	ii
FOREWORD	vii
INTRODUCTION	ix
1 Scope	1
2 Normative references	1
3 Terms, definitions, abbreviated terms, acronyms and conventions	1
3.1 Terms and definitions	1
3.2 Abbreviated terms and acronyms	6
3.3 Conventions	7
4 General principles	7
4.1 Concepts	7
4.2 Maturity model	9
5 Practice 1 – Security management	10
5.1 Purpose	10
5.2 SM-1: Development process	11
5.2.1 Requirement	11
5.3 Rationale and supplemental guidance	11
5.4 SM-2: Identification of responsibilities	11
5.4.1 Requirement	11
5.4.2 Rationale and supplemental guidance	11
5.5 SM-3: Identification of applicability	11
5.5.1 Requirement	11
5.5.2 Rationale and supplemental guidance	12
5.6 SM-4: Security expertise	12
5.6.1 Requirement	12
5.6.2 Rationale and supplemental guidance	12
5.7 SM-5: Process scoping	12
5.7.1 Requirement	12
5.7.2 Rationale and supplemental guidance	13
5.8 SM-6: File integrity	13
5.8.1 Requirement	13
5.8.2 Rationale and supplemental guidance	13
5.9 SM-7: Development environment security	13
5.9.1 Requirement	13
5.9.2 Rationale and supplemental guidance	13
5.10 SM-8: Controls for private keys	13
5.10.1 Requirement	13
5.10.2 Rationale and supplemental guidance	14
5.11 SM-9: Security requirements for externally provided components	14
5.11.1 Requirement	14
5.11.2 Rationale and supplemental guidance	14
5.12 SM-10: Custom developed components from third-party suppliers	15
5.12.1 Requirement	15
5.12.2 Rationale and supplemental guidance	15
5.13 SM-11: Assessing and addressing security-related issues	15
5.13.1 Requirement	15
5.13.2 Rationale and supplemental guidance	15
5.14 SM-12: Process verification	15
5.14.1 Requirement	15
5.14.2 Rationale and supplemental guidance	15
5.15 SM-13: Continuous improvement	16
5.15.1 Requirement	16

5.15.2	Rationale and supplemental guidance	16
6	Practice 2 – Specification of security requirements	17
6.1	Purpose	17
6.2	SR-1: Product security context	17
6.2.1	Requirement	17
6.2.2	Rationale and supplemental guidance	17
6.3	SR-2: Threat model	18
6.3.1	Requirement	18
6.3.2	Rationale and supplemental guidance	18
6.4	SR-3: Product security requirements	19
6.4.1	Requirement	19
6.4.2	Rationale and supplemental guidance	19
6.5	SR-4: Product security requirements content	19
6.5.1	Requirement	19
6.5.2	Rationale and supplemental guidance	19
6.6	SR-5: Security requirements review	20
6.6.1	Requirement	20
6.6.2	Rationale and supplemental guidance	20
7	Practice 3 – Secure by design	20
7.1	Purpose	20
7.2	SD-1: Secure design principles	20
7.2.1	Requirement	20
7.2.2	Rationale and supplemental guidance	21
7.3	SD-2: Defense in depth design	22
7.3.1	Requirement	22
7.3.2	Rationale and supplemental guidance	22
7.4	SD-3: Security design review	22
7.4.1	Requirement	22
7.4.2	Rationale and supplemental guidance	23
7.5	SD-4: Secure design best practices	23
7.5.1	Requirement	23
7.5.2	Rationale and supplemental guidance	23
8	Practice 4 – Secure implementation	24
8.1	Purpose	24
8.2	Applicability	24
8.3	SI-1: Security implementation review	24
8.3.1	Requirement	24
8.3.2	Rationale and supplemental guidance	24
8.4	SI-2: Secure coding standards	25
8.4.1	Requirement	25
8.4.2	Rationale and supplemental guidance	25
9	Practice 5 – Security verification and validation testing	25
9.1	Purpose	25
9.2	SVV-1: Security requirements testing	25
9.2.1	Requirement	25
9.2.2	Rationale and supplemental guidance	26
9.3	SVV-2: Threat mitigation testing	26
9.3.1	Requirement	26
9.3.2	Rationale and supplemental guidance	26
9.4	SVV-3: Vulnerability testing	27
9.4.1	Requirement	27
9.4.2	Rationale and supplemental guidance	27
9.5	SVV-4: Penetration testing	27
9.5.1	Requirement	27
9.5.2	Rationale and supplemental guidance	27
9.6	SVV-5: Independence of testers	28

9.6.1	Requirement	28
9.6.2	Rationale and supplemental guidance	28
10	Practice 6 – Management of security-related issues	29
10.1	Purpose	29
10.2	DM-1: Receiving notifications of security-related issues	29
10.2.1	Requirement	29
10.2.2	Rationale and supplemental guidance	29
10.3	DM-2: Reviewing security-related issues	30
10.3.1	Requirement	30
10.3.2	Rationale and supplemental guidance	30
10.4	DM-3: Assessing security-related issues	30
10.4.1	Requirement	30
10.4.2	Rationale and supplemental guidance	30
10.5	DM-4: Addressing security-related issues	31
10.5.1	Requirement	31
10.5.2	Rationale and supplemental guidance	32
10.6	DM-5: Disclosing security-related issues	32
10.6.1	Requirement	32
10.6.2	Rationale and supplemental guidance	33
10.7	DM-6: Periodic review of security defect management practice	33
10.7.1	Requirement	33
10.7.2	Rationale and supplemental guidance	33
11	Practice 7 – Security update management	33
11.1	Purpose	33
11.2	SUM-1: Security update qualification	33
11.2.1	Requirement	33
11.2.2	Rationale and supplemental guidance	34
11.3	SUM-2: Security update documentation	34
11.3.1	Requirement	34
11.3.2	Rationale and supplemental guidance	34
11.4	SUM-3: Dependent component or operating system security update documentation	34
11.4.1	Requirement	34
11.4.2	Rationale and supplemental guidance	34
11.5	SUM-4: Security update delivery	35
11.5.1	Requirement	35
11.5.2	Rationale and supplemental guidance	35
11.6	SUM-5: Timely delivery of security patches	35
11.6.1	Requirement	35
11.6.2	Rationale and supplemental guidance	35
12	Practice 8 – Security guidelines	35
12.1	Purpose	35
12.2	SG-1: Product defense in depth	36
12.2.1	Requirement	36
12.2.2	Rationale and supplemental guidance	36
12.3	SG-2: Defense in depth measures expected in the environment	36
12.3.1	Requirement	36
12.3.2	Rationale and supplemental guidance	36
12.4	SG-3: Security hardening guidelines	37
12.4.1	Requirement	37
12.4.2	Rationale and supplemental guidance	37
12.5	SG-4: Secure disposal guidelines	38
12.5.1	Requirement	38
12.5.2	Rationale and supplemental guidance	38
12.6	SG-5: Secure operation guidelines	38
12.6.1	Requirement	38
12.6.2	Rationale and supplemental guidance	38
12.7	SG-6: Account management guidelines	38

12.7.1	Requirement.....	39
12.7.2	Rationale and supplemental guidance.....	39
12.8	SG-7: Documentation review.....	39
12.8.1	Requirement.....	39
12.8.2	Rationale and supplemental guidance.....	39
Annex A	(informative) Possible metrics.....	40
Annex B	(informative) Table of requirements.....	42
Bibliography		44

List of Figures

Figure 1	— Parts of the IEC 62443 series.....	x
Figure 2	— Example scope of product life-cycle.....	xi
Figure 3	— Defence in depth strategy is a key philosophy of the secure product life-cycle.....	8

List of Tables

Table 1	— Maturity levels.....	9
Table 2	— Example SDL continuous improvement activities.....	16
Table 3	— Required level of independence of testers from developers.....	28
Table B.1	— Summary of all requirements.....	42

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](#).

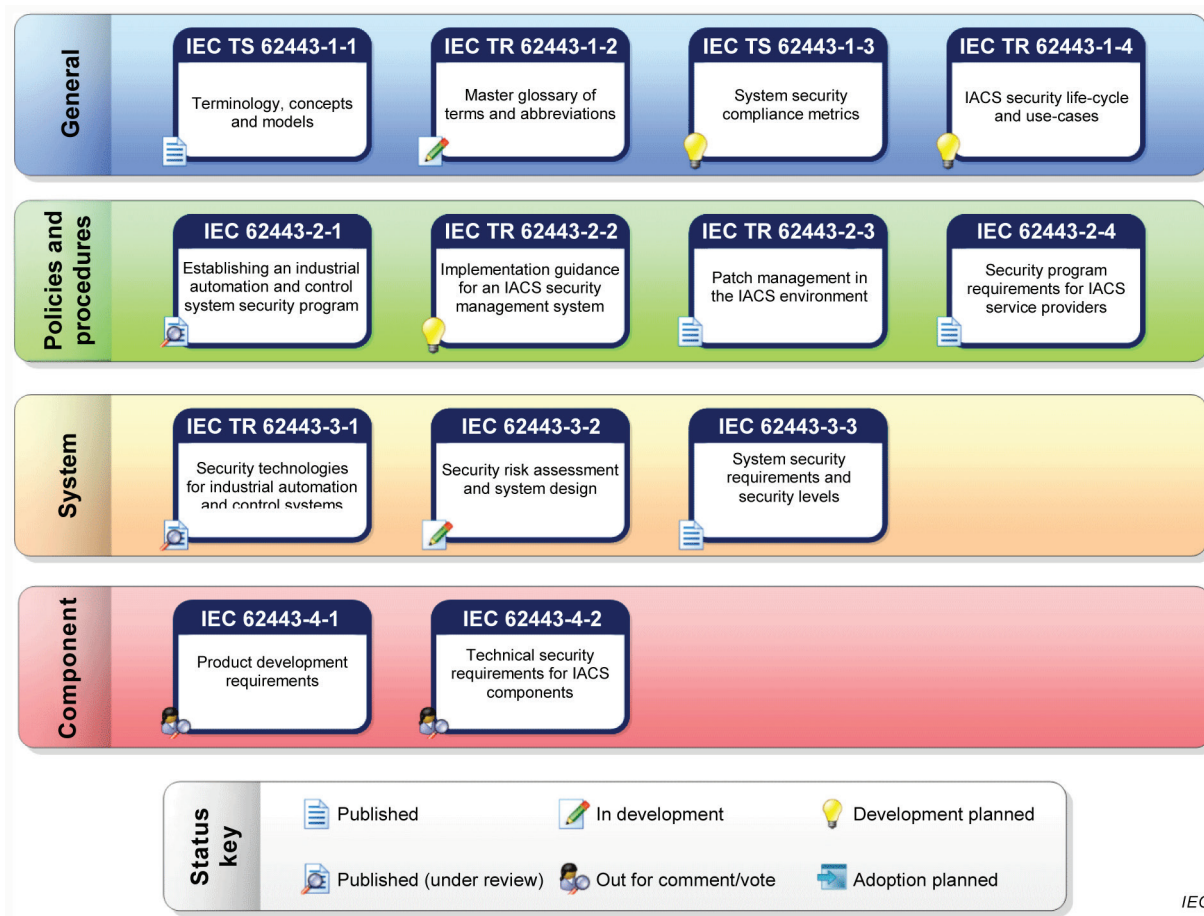


Figure 1 — Parts of the IEC 62443 series

[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.

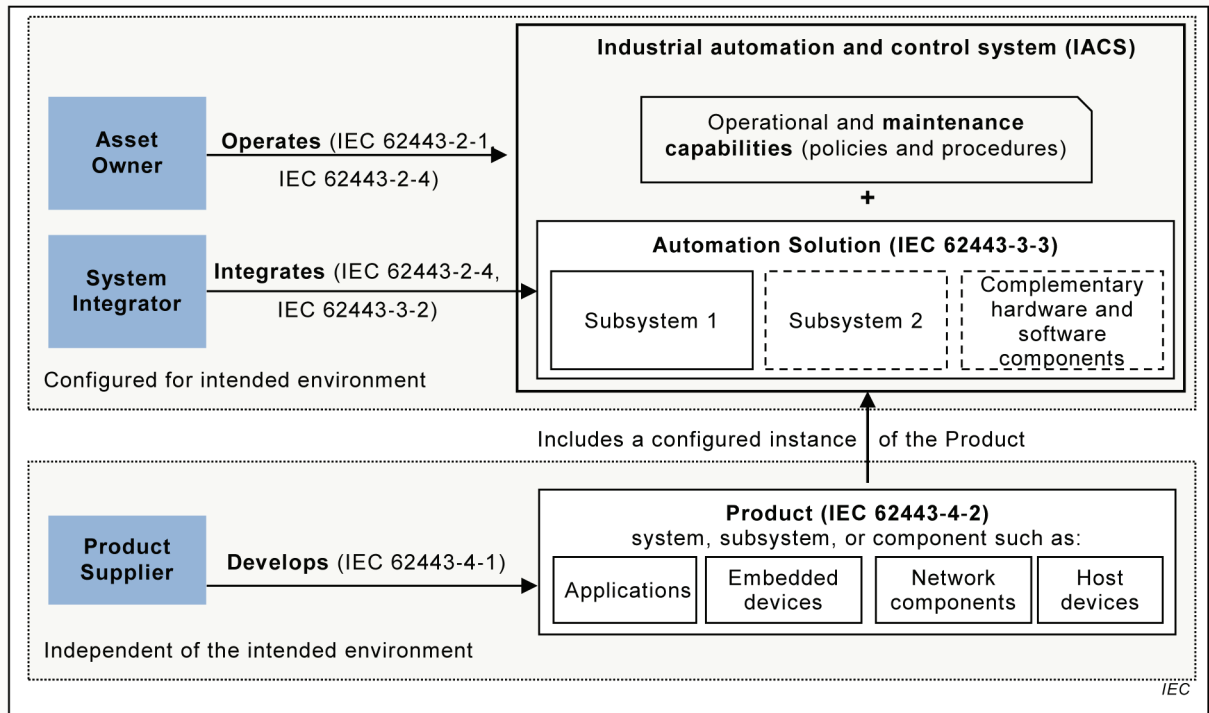


Figure 2 — Example scope of product life-cycle

NOTES

Australian Standard®

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 62443-1-2²⁾ 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

2) Under consideration.

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 IEC 62443 series.

3.1.4

administrator

user who has been authorized to manage security policies/capabilities for a product or system

3.1.5

asset

physical or logical object owned by or under the custodial duties of an organization, having either a perceived or actual value to the organization

Note 1 to entry: In this specific case, an asset is an object that is part of an [IACS](#).

3.1.6

asset owner

individual or organization responsible for one or more IACSS

3.1.7

attack surface

physical and functional interfaces of a system that can be accessed and, therefore, potentially exploited by an attacker

3.1.8

audit log

event log that requires a higher level of integrity protection than provided by typical event logs

Note 1 to entry: Audit logs are used to protect against claims that repudiate responsibility for an action.

3.1.9

authentication

provision of assurance that a claimed characteristic of an identity is correct

Note 1 to entry: Not all credentials used to authenticate an identity are created equally. The trustworthiness of the credential is determined by the configured authentication mechanism. Hardware or software-based mechanisms can force users to prove their identity before accessing data on a device. A typical example is proving the identity of a user usually through an identity provider.

Note 2 to entry: Authentication includes verifying human users as well as non-human users such as devices or processes.

3.1.10

automation solution

control system and any complementary hardware and software components that have been installed and configured to operate in an [IACS](#)

Note 1 to entry: Automation Solution is used as a proper noun in this part of the IEC 62443 series.

Note 2 to entry: The difference between the control system and the Automation Solution is that the control system is incorporated into the Automation Solution design (for example, a specific number of workstations, controllers and devices in a specific configuration), which is then implemented. The resulting configuration is referred to as the Automation Solution.

Note 3 to entry: The Automation Solution can be comprised of components from multiple suppliers including the product supplier of the control system.

3.1.11**banned function**

software method that is no longer recommended to be used in software because more secure versions exist with less propensity for misuse

Note 1 to entry: Banned functions are sometimes called banned methods or banned Application Programming Interfaces (APIs).

3.1.12**best practices**

guidelines for securely designing, developing, testing, maintaining or retiring products that the supplier has determined are commonly recommended by both the security and industrial automation communities

EXAMPLE Least privilege, economy of mechanism and least common mechanism.

3.1.13**component**

one of the parts that make up a product or system

Note 1 to entry: A component may be hardware or software and may be subdivided into other components.

3.1.14**configuration management**

discipline of identifying the components of an evolving system for the purposes of controlling changes to those components and maintaining continuity and traceability throughout the life-cycle

3.1.15**defense in depth**

approach to defend the system against any particular attack using several independent methods

Note 1 to entry: Defense in depth implies layers of security and detection, even on single systems, and provides the following features:

- is based on the idea that any one layer of protection, may and probably will be defeated;
- attackers are faced with breaking through or bypassing each layer without being detected;
- a flaw in one layer can be mitigated by capabilities in other layers;
- system security becomes a set of layers within the overall network security; and
- each layer should be autonomous and not rely on the same functionality nor have the same failure modes as the other layers.

3.1.16**dependent component**

component external to the product on which the product depends

EXAMPLE Java run time environment or a driver

Note 1 to entry: This includes both hardware and software.

3.1.17**deprecated function**

software method that is supported but whose use is no longer recommended

Note 1 to entry: Methods are generally deprecated before becoming obsolete (deleted from the set of functions provided by the supplier of the function). Deprecated functions are sometimes called deprecated methods or deprecated APIs.

3.1.18**externally provided component**

component included in a product that is developed by an external organization and is not developed specifically for one supplier

Note 1 to entry: Examples include purchased software and open source software.

3.1.19**fuzz testing**

process of creating malformed or unexpected data or call sequences to be consumed by the entity under test to verify that they are handled appropriately

3.1.20**industrial automation and control system**

collection of personnel, hardware, software, procedures and policies involved in the operation of the industrial process and that can affect or influence its safe, secure and reliable operation

Note 1 to entry: The [IACS](#) can include components that are not installed at the asset owner's site.

Note 2 to entry: The definition of [IACS](#) was taken from in IEC 62443-3-3 [\[10\]](#) and is illustrated in [Figure 2](#).

3.1.21**patch management**

area of systems management that involves acquiring, testing and installing software patches (code changes) to a product

Note 1 to entry: See IEC TR 62443-2-3 [\[7\]](#) for additional information.

Note 2 to entry: Patch management also applies to the process of keeping included 3rd party libraries current before releasing a product.

3.1.22**product**

system, subsystem or component that is manufactured, developed or refined for use by other products

Note 1 to entry: The processes required by the practices defined in this document apply iteratively to all levels of product design (for example, from the system level to the component level).

3.1.23**product security context**

security provided to the product by the environment (asset owner deployment) in which the product is intended to be used

Note 1 to entry: The security provided to the product by its intended environment can effectively restrict the threats that are applicable to the product.

3.1.24**product supplier**

manufacturer of hardware and/or software product

Note 1 to entry: The product supplier includes the entity responsible for developing and maintaining a product which can include more than just the manufacturer (for example, integrator).

3.1.25**product users**

users of the hardware and/or software product including asset owners, integrators and maintenance personnel, vendors of other components or products that reuse or contain this product

3.1.26**record**

document stating results achieved or providing evidence of activities performed

Note 1 to entry: The term artefact is often used to have the same meaning.

3.1.27**regression**

change to a system component that has adversely affected functionality, reliability or performance or has introduced additional defects

3.1.28**root cause**

initiating cause of either a condition or a causal chain that leads to an outcome or effect of interest

Note 1 to entry: These weaknesses often result from misapplication of best practices.

3.1.29**security defect**

design or implementation deficiency that can be exploited to compromise an asset or resource

3.1.30**security advisor**

organizational role to guide team in the process of the [SDL](#) (Security Development Life-cycle)

Note 1 to entry: Security advisor may be part of the project team or may be consultant to the team to provide guidance and assistance where required.

3.1.31**security incident**

security compromise that is of some significance to the asset owner or failed attempt to compromise the system whose result could have been of some significance to the asset owner

Note 1 to entry: The term “near miss” is sometimes used to describe an event that could have been an incident under slightly different circumstances.

3.1.32**security-related issue**

characteristic of the design or implementation of the product that can potentially affect the security of the product

3.1.33**security verification and validation testing**

testing performed to assess the overall security of a component, product or system when used in its intended product security context and to determine if a component, product or system satisfies the product security requirements and satisfies its designed security purpose

Note 1 to entry: Security verification testing supplements security validation testing with additional testing focused on the product security context and defense in depth strategy.

3.1.34**system integrator**

person or company that specializes in bringing together component subsystems into a whole and ensuring that those subsystems perform in accordance with project specifications

3.1.35**third party supplier**

organization independent of the product supplier organization