



DPC: 25 / 30509463 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 31 January 2025

Origin: International

Latest date for receipt of comments: 19 February 2025

Project No. 2025/00346

Responsible committee: GEL/65 Measurement and control

Interested committees:

Title: BS EN IEC 62443-1-1 Security for automation and control systems

Part 1-1: Overview and Guidance for the IEC 62443 Series

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

**WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD.
THIS DRAFT IS NOT CURRENT BEYOND 19 February 2025**

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <http://standardsdevelopment.bsigroup.com>

Responsible Committee Secretary: Ms Charmaine Mukherjee (BSI)

Direct tel:

E-mail: charmaine.mukherjee@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/Figure/ Table/Note	Type of comment	Commend (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



65/1112/CD

COMMITTEE DRAFT (CD)

PROJECT NUMBER:

IEC 62443-1-1 ED1

DATE OF CIRCULATION:

2025-01-24

CLOSING DATE FOR COMMENTS:

2025-03-21

SUPERSEDES DOCUMENTS:

65/1110/RR

IEC TC 65 : INDUSTRIAL-PROCESS MEASUREMENT, CONTROL AND AUTOMATION

SECRETARIAT:

France

SECRETARY:

Mr Didier GIARRATANO

OF INTEREST TO THE FOLLOWING COMMITTEES:

TC 9,TC 22,TC 23,SC 23B,SC 23K,TC 34,TC 44,TC 45,TC 57,TC 61,TC 62,SC 62A,TC 69,TC 72,TC 80,TC 82,TC 88,TC 121,SC 121A,SC 121B,TC 124

HORIZONTAL FUNCTION(S):

TC 65 Horizontal Security

ASPECTS CONCERNED:

Information security and data privacy

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Recipients of this document are invited to submit, with their comments, notification of any local regulations or technical reasons that may exist and should be considered should this proposal proceed, recognizing that failure to address such requirements could result in the need for new or existing "In Some Countries" clauses. (SEE [AC/22/2007](#) OR [NEW GUIDANCE DOC](#)).

TITLE:

Security for automation and control systems – Part 1-1: Overview and Guidance for the IEC 62443 Series

NOTE FROM TC/SC OFFICERS:

Copyright © 2025 International Electrotechnical Commission, IEC. All rights reserved. It is permitted to download this electronic file, to make a copy and to print out the content for the sole purpose of preparing National Committee positions. You may not copy or "mirror" the file or printed version of the document, or any part of it, for any other purpose without permission in writing from IEC.

CONTENTS

1		
2	FOREWORD	5
3	INTRODUCTION	7
4	1 Scope	8
5	1.1 Scope of the IEC 62443 Series	8
6	1.2 Scope of this document	8
7	2 Normative References	9
8	3 Terms, definitions, and abbreviations	9
9	3.1 Terms and Definitions	9
10	3.2 Abbreviated terms and acronyms	25
11	4 Case for Action (Informative)	27
12	4.1 General	27
13	4.2 Business Context	27
14	4.3 Current Systems	27
15	4.4 Influences	28
16	4.5 Potential Consequences	28
17	4.6 Impact of Security Measures	28
18	5 Overview of the IEC 62443 Series	29
19	5.1 General	29
20	5.2 ACS Security	29
21	5.3 Series Structure	29
22	5.4 Requirements Structure	31
23	5.5 Evolved Concepts	32
24	6 Use of the IEC 62443 standards	33
25	6.1 General	33
26	6.2 Principal Roles	33
27	6.3 Roles and Standards	34
28	6.4 Other Roles	36
29	6.5 Profiles	36
30	7 Security Programs	37
31	7.1 General	37
32	7.2 Maturity Levels	38
33	7.3 Security Protection Scheme	39
34	7.4 Security Protection Rating	40
35	8 Security Risk Assessment	40
36	8.1 General	40
37	8.2 Risk-Based Approach	40
38	8.3 ACS Security Imperatives	40
39	8.4 Equipment Under Control (EuC)	41
40	8.5 Security Zones and Conduits	42
41	8.6 Security Levels	44
42	8.7 Essential functions	45
43	8.8 Compensating Security Measures	45
44	8.9 Security and Functional Safety	45
45	9 Security Lifecycles	47
46	9.1 General	47

65/1112/CD

47	9.2	Standards by Lifecycle	47
48	9.3	Product Development Lifecycle.....	48
49	9.4	ACS Lifecycle	48
50	10	General Security Concepts.....	49
51	10.1	General	49
52	10.2	Security Activities	50
53	10.3	Least Privilege.....	51
54	10.4	Least function.....	51
55	10.5	Defense-in-Depth	51
56	10.6	Supply chain security.....	51
57		Annex A – Rationale for Changes to Terms and Concepts	53
58	A.1	Introduction	53
59	A.2	Qualifying the Series as Industrial	53
60	A.3	Deprecated terms	54
61	A.4	Series Term Ontologies	54
62	A.5	Automation and control solution.....	55
63	A.6	Security program	56
64	A.7	Security measure.....	57
65	A.8	Automation and control system (ACS)	58
66		Bibliography	60

67

FIGURES

69	Figure 1 – Series Parts by Principal Role	34
70	Figure 2 – Roles and Responsibilities Overview	36
71	Figure 3 – Security Program Categories	37
72	Figure 4 – Lifecycle Linkages	47
73	Figure 5 – Standards by Lifecycle.....	48
74	Figure 6 – ACS Lifecycle	49
75	Figure 7 – Security Context Map	50
76	Figure A.1 – Asset ontology.....	55
77	Figure A.2 – Automation and Control Solution ontology	56
78	Figure A.3 – Security Program ontology	57
79	Figure A.4 – Security measure ontology	58
80	Figure A.5 – System - Component - Function model	59

81

TABLES

83	Table 1 – Published parts of the IEC 62443 series	29
84	Table 2 – Foundational Requirements	31
85	Table 3 – Security Program Elements.....	32
86	Table 4 – Conformance Standards by Principal Role	35
87	Table 5 – Maturity level	39
88	Table 6 – Comparison of Functional Safety and ACS Cyber Security.....	46
89	Table 7 – Representative Lifecycle Stages	47

90	Table 8 – ACS Lifecycle Stages.....	49
91	Table A.1 – Deprecated Series Terms	54
92		
93		
94		

INTERNATIONAL ELECTROTECHNICAL COMMISSION

SECURITY FOR AUTOMATION AND CONTROL SYSTEMS –

Part 1-1: Overview and Guidance for the IEC 62443 Series

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) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at <https://patents.iec.ch>. IEC shall not be held responsible for identifying any or all such patent rights.
- IEC 62443-1-1 has been processed by IEC technical committee 65: Industrial-process measurement, control and automation. IEC 62443-1-1 has been developed by IEC TC 65 and the liaison ISA99: ISA committee on Security for industrial automation and control systems.

The text of this standard is based on the following document:

This standard was approved for publication by the P-members of the committee concerned as indicated in the following document

Draft	Report on voting
XX/XX/	XX/XX/

This page intentionally left blank

INTRODUCTION

Intended Audience

The intended audience for this standard includes asset owners, product suppliers, service providers, and, where appropriate, conformance bodies and compliance authorities. Compliance authorities include but are not limited to government agencies and regulators with the legal authority to perform audits to verify compliance with governing laws and regulations.

Objective

The objective of automation and control systems security is to reduce the risk of cyber issues causing personal injury, impacting physical or logical assets, or endangering public health, losing public or consumer confidence, disclosing sensitive information assets, failing to protect business assets, or failing to comply with regulations. These concepts are applied to any automation and control system in the automated process and include both stand-alone and networked components. Communications between automation and control systems may be either through internal messaging or by any human or machine interfaces that authenticate, operate, control, or exchange data with any of these automation and control systems.

The IEC 62443 series

The IEC 62443 series includes standards, specifications, and reports that address the need to address security robustness and resilience in the design, implementation, and operation of automation and control systems (ACS).

Robustness provides the capabilities for the equipment under control (EuC) to operate under a range of cyber-induced perturbations and disturbances. To resist cyber-induced errors, as opposed to random errors, the automation and control systems must also be resilient. Resilience provides the capabilities to restore normal operation after unexpected cyber-induced events. Robustness and resilience are not general properties of an ACS but are relevant to specific classes of perturbations. An ACS that is resilient or robust to a certain type of cyber-induced perturbations may be brittle or fragile to another.

The purpose of the IEC 62443 series is to improve the safety, integrity, availability, and confidentiality of components of an ACS, and to provide criteria for procuring and implementing a secure ACS. Application of the requirements and guidance in the IEC 62443 series will improve cyber security and help to reduce the risk of compromising the equipment under control or sensitive information.

The IEC 62443 series complements established standards for the security of information technology systems (e.g., ISO/IEC 27000) by identifying and addressing the important differences present in an ACS. Many of these differences are based on the reality that an ACS controls physical processes. Resulting cyber security risks with ACS may have health, safety, or environment (HSE) implications and the response should be integrated with other existing risk management practices addressing these risks. Each of the individual standards and reports in the IEC 62443 series addresses a specific aspect of the subject.

SECURITY FOR AUTOMATION AND CONTROL SYSTEMS –

Part 1-1: Overview and Guidance for the IEC 62443 Series

1 Scope

1.1 Scope of the IEC 62443 Series

The range of application of the series is not limited to specific industries or sectors but is defined in terms of potential consequences. Specifically, the scope of this series is automation systems whose compromise could result in any or all the following consequences, irrespective of the industry:

- Endangerment of the public or employee safety or health.
- Damage to the environment.
- Damage to the equipment under control.
- Disruption in the operation of the equipment under control.
- Loss of product integrity.
- Loss of public confidence or company reputation.
- Violation of legal or regulatory requirements.
- Financial loss.
- Loss of proprietary or confidential information.

1.2 Scope of this document

The scope of this document is the set of main cybersecurity elements (i.e., terms, figures, requirements, and concepts) that apply to the IEC 62443 series and notably those that appear in two or more parts of the series. These are the foundation of the series. Each of these elements is described in more detail in subsequent parts in the series.

65/1112/CD

2 Normative References

The following referenced documents are indispensable for the application of this standard.

ANSI/ISA-95.00.01-2000, *Enterprise-control system integration - Part 1: Models and terminology*

3 Terms, definitions, and abbreviations

3.1 Terms and Definitions

The following are the series terms¹ for the IEC 62443 series.

In addition, ISO and IEC maintain terminology databases for use in standardization at the following addresses:

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

3.1.1 access

ability and means to communicate with or otherwise interact with a system to use system resources

Note 1 to entry: Access may involve physical access (authorization to be allowed physically in an area, possession of a physical key lock, PIN code, or access card or biometric attributes that allow access) or logical access (authorization to log into to a system and application, through a combination of logical and physical means).

3.1.2 access control

protection of system resources against unauthorized access

Note 1 to entry: A process by which the use of system resources is regulated according to a security policy and is permitted by only authorized entities (users, programs, processes, or other systems) according to that policy.

3.1.3 accountability

property of a system (including all of its system resources) that ensures that the actions of a system entity may be traced uniquely to that entity, which can be held accountable for its actions

3.1.4 ACS environment

collection of systems and associated infrastructure within which the ACS operates

3.1.5 actuating function

changes the state of a physical property

EXAMPLE Current, flow, humidity, light, liquid level, position, pressure, temperature, or velocity.

3.1.6 actuator

hardware and software that causes a change through the direct control of physical devices and systems, processes, and events

3.1.7 alarm system

a type of automation and control system that provides sensing and view functions

EXAMPLE Fire alarm system, process alarm system, intrusion alarm system, gas detection alarm system

¹ Series terms are defined as main terms that apply to the 62443 series and notably those that appear in two or more parts of the series.

3.1.8**application**

software program that performs specific functions initiated by a user command or a process event and that can be executed without access to system control, monitoring, or administrative privileges

3.1.9**application component**

one or more software programs and their dependencies that provides one or more component functions

EXAMPLE Control applications, implementation and test applications, record analyze and report applications, safety applications, security utility applications.

Note 1 to entry: Application components typically execute on platform components, but may also execute on embedded components or communication components.

Note 2 to entry: Application dependencies are any software programs that are necessary for the application to function, such as database packages, reporting tools, or any commercial 3rd party or open-source software.

Note 3 to entry: Application components may also include container support and orchestration applications.

3.1.10**area**

a subset of a site's physical, geographic, or logical group of assets

Note 1 to entry: An area may contain manufacturing lines, process cells, and production units.

Note 2 to entry: Areas may be connected by a local area network on site and may contain systems related to the operations performed in that area.

3.1.11**asset**

physical or logical entity that has perceived or actual value to an organization

3.1.12**asset operator**

entity that is responsible for the operation of one or more industrial automation and control systems

3.1.13**asset owner**

role of an organization that is accountable and responsible for one or more automation and control solutions and the associated equipment under control

Note 1 to entry: The asset owner role includes the operator of the automation and control solution and the associated equipment under control.

3.1.14**attack**

assault on a system that derives from an intelligent threat

Note 1 to entry: An intelligent threat is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Note 2 to entry: There are four different commonly recognized classes of attack: An 'active attack' attempts to alter system resources or affect their operation. A 'passive attack' attempts to learn or make use of information from the system but does not affect system resources. An 'inside attack' is an attack initiated by an entity inside the security perimeter (an 'insider') – That is, an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization. An 'outside attack' is initiated from outside the perimeter by an unauthorized or illegitimate user of the system (including an insider attacking from outside the security perimeter). Potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments.

3.1.15**audit**

independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend changes in security measures, policies, or procedures

Note 1 to entry: There are three forms of audit. (1) External audits conducted by parties who are not employees or permanent contractors of the organization. (2) Internal audits conducted by a separate organizational unit dedicated

65/1112/CD

to internal auditing. (3) Security measure assessments conducted by peer members of the process automation function.

3.1.16

authentication

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

3.1.17

authentication domain

environment or context that is defined by a security policy, security model, or security architecture to include a set of system resources and the set of system entities that have the right to access the resources

3.1.18

authorization

right or a permission that is granted to a system entity to access a system resource

3.1.19

automation and control solution

collection of people, processes, and automation and control systems with the purpose of monitoring, controlling, and managing the operation of the equipment under control

Note 1 to entry: An automation and control solution includes the instantiation of one or more automation and control systems.

3.1.20

automation and control system

interacting collection of related components that provide functions for monitoring and controlling the operation of equipment under control

Note 1 to entry: The automation and control system includes, but is not limited to: actuating function, control function, data flow control function, history function, hosting function, manipulating function, safety function, sensing function, view function, utility function (security, management), and view function.

3.1.21

automation solution

see Automation and Control Solution

3.1.22

automation system

See automation and control system

3.1.23

availability

property of ensuring timely and reliable access to and use of control system information and functionality

3.1.24

business system

collection of information technology elements (i.e., hardware, software, and services) installed with the intent to facilitate an organization's business process or processes (administrative or project)

3.1.25

capability security level

security level inherent in a product or technology

Note 1 to entry: Capability security level is determined during the product development phase of the security lifecycle.

3.1.26

cell

lower-level element of a manufacturing process that performs manufacturing, field device control, or vehicle functions

Note 1 to entry: Entities at this level may be connected by an area control network and may contain information systems related to the operations performed in that entity.

3.1.27**change management**

See management of change

3.1.28**channel**

See data flow

3.1.29**client**

device or application receiving or requesting services or information from a server

3.1.30**code**

character or bit pattern that is assigned a particular meaning to express a computer program in a programming language.

Note 1 to entry: Source codes are instructions and data definitions expressed in a form suitable for input to an assembler, compiler, or other translator.

Note 2 to entry: Coding is the process of expressing logic and data from design specifications or descriptions into a programming language.

Note 3 to entry: A programming language is a language used to express computer programs.

[SOURCE: IEC 62628, ed. 1.0 (2012-08)]

3.1.31**communication component**

physical or virtual component whose primary purpose is to facilitate or restrict data flow between components

EXAMPLE Network switch, network router, software defined network, virtual LAN.

3.1.32**communication path**

logical connection between a source and one or more destinations

Note 1 to entry: Destinations could be devices, physical processes, data items, commands, or programmatic interfaces.

Note 2 to entry: The communication path is not limited to wired or wireless networks, but includes other means of communication such as memory, procedure calls, state of the physical plant, portable media, and human interactions.

3.1.33**communication system**

arrangement of hardware, software, and propagation media to allow the transfer of messages from one application to another

3.1.34**compensating countermeasure**

see compensating security measure

3.1.35**compensating security measure**

security measure employed in lieu of or in addition to inherent security capabilities to satisfy one or more security requirements

3.1.36**compliance authority**

individual or organization verifying compliance with a specification, policy, or standard

3.1.37**component**

hardware, software or both with the capability to provide one or more functions to a system

EXAMPLE Application component, embedded component, communication component, and platform component

Note 1 to entry: A component may have multiple component types.

65/1112/CD

Note 2 to entry: Components can be either physical (e.g. sensor) or virtual (e.g. software defined network).

Note 3 to entry: A component may be packaged as a product.

3.1.38

conduit

see security conduit

Note 1 to entry: See security conduit.

3.1.39

confidentiality

assurance that information is not disclosed to unauthorized individuals, processes, or devices

3.1.40

control center

central location used to operate the equipment under control

Note 1 to entry: Infrastructure industries typically use one or more control centers to supervise or coordinate their operations. If there are multiple control centers (e.g., a backup center at a separate site), they are typically connected via a wide area network. The control center contains the host computers and associated operator display devices plus ancillary information systems such as a historian.

Note 2 to entry: In some industries, the term “control room” may be more commonly used.

Note 3 to entry: Control systems do not require that there be a control center.

3.1.41

control function

automatic regulation of one or more outputs based on one or more inputs

EXAMPLE PID control, sequential control, discrete control, event control, multivariable predictive control.

3.1.42

control network

a time-critical network that is typically connected to equipment that controls physical processes

Note 1 to entry: The control network can be subdivided into segments.

Note 2 to entry: There can be multiple separate control networks within one company or site.

3.1.43

control system

a type of automation and control system that provides the control function

EXAMPLE Distributed Control System (DCS), Industrial Control System (ICS), Supervisory Control and Data Acquisition (SCADA) system.

3.1.44

countermeasure

See security measure.

3.1.45

cryptographic algorithm

algorithm based on encryption algorithms, cryptographic hash algorithms, digital signature algorithms, and key agreement algorithms

3.1.46

cryptographic key

input parameter that varies the transformation performed by a cryptographic algorithm

Note 1 to entry: This term is usually shortened to just ‘key.’

3.1.47

cybersecurity

actions required to preclude unauthorized use of, denial of service to, modifications to, disclosure of, or damage to systems or informational assets

Note 1 to entry: Cybersecurity includes the concepts of identification, authentication, accountability, authorization, availability, privacy, and confidentiality.

3.1.48**data confidentiality**

property that information is not made available or disclosed to any unauthorized system entity, including unauthorized individuals, entities, or processes

3.1.49**data flow**

movement of data through an Automation and Control Solution, system or component

3.1.50**data flow control function**

ability to manage data flows

Note 1 to entry: Includes supporting and restricting data flows.

3.1.51**decryption**

process of changing ciphertext into plaintext using a cryptographic algorithm and key

3.1.52**defense-in-depth**

provision of multiple security measures, especially in layers, with the intent to prevent or delay an attack

Note 1 to entry: Also written as defense-in-depth.

3.1.53**demilitarized zone**

common, limited network of servers joining two or more zones to control data flow between zones

Note 1 to entry: The purpose of a DMZ is to enforce the internal network's policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal network from outside attacks.

Note 2 to entry: In the context of automation and control systems, the term "internal network" is typically applied to the network or segment that is the primary focus of protection. For example, a control network could be considered "internal" when connected to an "external" business network.

Note 3 to entry: DMZ is typically located between the IT and OT systems.

3.1.54**denial of service**

prevention or interruption of authorized access to a system resource or the delaying of system operations and functions

Note 1 to entry: In the context of automation and control systems (ACSs), denial of service (DoS) can refer to the loss of process function, not just the loss of data communications.

3.1.55**device**

hardware manifestation of one or more components

EXAMPLE Embedded device, network device, host device.

3.1.56**digital signature**

result of a cryptographic transformation of data which, when properly implemented, provides the services of origin authentication, data integrity, and signer non-repudiation

3.1.57**eavesdropping**

monitoring or recording of communicated information by unauthorized parties

3.1.58**embedded component**

physical component which has one or more of the functions actuating, control, safety, sensing, or view or manipulate, and may host one or more applications

65/1112/CD

Note 1 to entry: Attributes include limited storage, limited computational resources, limited number of exposed services, programmed through an external interface, embedded operating systems (OSs) or firmware equivalent, real-time scheduler, may have an attached control panel, and may have a communications interface.

3.1.59

embedded device

hardware manifestation of an embedded component

3.1.60

encryption

cryptographic transformation of plaintext into ciphertext that conceals the data's original meaning to prevent it from being known or used

Note 1 to entry: See "decryption."

3.1.61

enterprise

one or more organizations sharing a definite mission, goals and objectives which provides an output such as product or service.

[SOURCE: IEC 62264-1:2013]

3.1.62

equipment under control

equipment, machinery, apparatus, or plant used for manufacturing, process, transportation, medical, or other activities

[SOURCE: IEC 61508-4:2010]

3.1.63

essential function

function or capability that is required to maintain health, safety, the environment, and availability of the equipment under control

Note 1 to entry: Essential functions include, but are not limited to, the safety function, the control function, the view function, and the manipulate function. The asset owner may add additional essential functions.

Note 2 to entry: The loss of essential functions is commonly termed loss or protection, loss of control, or loss of view.

3.1.64

firewall

hardware device or software package that provides filtering and/or provision of rules to allow or deny specific types of network traffic to flow between zones

Note 1 to entry: A firewall is a type of security enforcement point.

Note 2 to entry: A firewall may be either an application installed on a general-purpose computer or a dedicated platform (appliance) that forwards or rejects/drops packets on a network. Typically, firewalls are used to protect zone boundaries and generally have rules restricting which ports and protocols are open.

3.1.65

foundational requirement

requirement that provides a basis for technical requirements in all standards in the IEC 62443 series

3.1.66

function

group of related actions with an intended purpose

Note 1 to entry: A function is a property of a component or system.

Note 2 to entry: A function may be implemented as a computing service.

3.1.67

gateway

relay mechanism that attaches to two (or more) computer networks that have similar functions but dissimilar implementations and that enables host computers on one network to communicate with hosts on the other

416 Note 1 to entry: A gateway is also described as an intermediate system that is the translation interface between two
417 computer networks.

418 **3.1.68**

419 **geographic site**

420 subset of an enterprise's physical, location-based, or logical group of assets

421 Note 1 to entry: A geographic site may contain areas, manufacturing lines, process cells, process units, control
422 centers, and vehicles, and it may be connected to other sites by a wide area network.

423 **3.1.69**

424 **history function**

425 ability to record, analyze, and report information

426 **3.1.70**

427 **host**

428 computer attached to a communication subnetwork or internetwork that can use services
429 provided by the network to exchange data with other attached computers

430 **3.1.71**

431 **host device**

432 hardware manifestation of a platform component with hosting function

433 **3.1.72**

434 **hosting function**

435 ability to execute additional functions not present in the original component

436 EXAMPLE Hypervisor, general purpose operating system, container engine

437 Note 1 to entry: Additional functions may come from a 3rd party.

438 Note 2 to entry: Hosting function may reside on platform, network, or embedded components.

439 **3.1.73**

440 **implemented security level**

441 security level of an automation solution that is designed and implemented based on the security
442 requirements specified by the asset owner

443 Note 1 to entry: Implemented security level is determined during the integration phase of the security lifecycle.

444 **3.1.74**

445 **information technology**

446 technology for gathering, storing, retrieving, processing, analyzing and transmitting information

447 [SOURCE: ISO 9241-20:2008, 3.4, modified – While the source entry is
448 information/communication technology, the definition was taken unmodified.]

449 **3.1.75**

450 **insider**

451 `trusted` person, employee, contractor, or supplier who has information that is not generally
452 known to the public

453 Note 1 to entry: See `outsider.`

454 **3.1.76**

455 **integration service provider**

456 service provider that provides integration activities for an automation and control solution

457 Note 1 to entry: Integration activities include design, installation, configuration, testing, commissioning, and
458 handover.

459 Note 1 to entry: Integration services providers are often referred to as system integrators or main automation
460 contractors (MAC).

461 **3.1.77**

462 **integrity**

463 state that connectivity, control, or safety have not been changed, destroyed or lost in an
464 unauthorized or accidental manner

65/1112/CD

3.1.78

interception

capture and disclosure of message contents or use of traffic analysis to compromise the confidentiality of a communication system based on message destination or origin, frequency or length of transmission, and other communication attributes

3.1.79

interface

logical entry or exit point that provides access to the module for logical information flows

3.1.80

intrusion

unauthorized act of compromising a system

Note 1 to entry: See `attack.`

3.1.81

intrusion detection

security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of attempts to access system resources in an unauthorized manner

3.1.82

key management

process of handling and controlling cryptographic keys and related material (such as initialization values) during their lifecycle in a cryptographic system

Note 1 to entry: The life cycle includes ordering, generating, distributing, storing, loading, escrowing, archiving, auditing, and destroying the keys and related material.

3.1.83

least functionality

security principle that the functionality of a system or component is restricted to the minimum necessary to accomplish required capabilities

Note 1 to entry: System hardening is the process to disable or remove functionality to achieve least functionality.

3.1.84

least privilege

security principle that a system or component restricts the access privileges of users to the minimum necessary to accomplish assigned tasks

3.1.85

lifecycle

evolution of a system, product, service, project, or other human-made entity from conception through retirement

[SOURCE: ISO/IEC/IEEE24748-1:2018]

3.1.86

line

lower-level element of a manufacturing process that performs manufacturing, field device control, or vehicle functions

Note 1 to entry: See `cell.`

3.1.87

maintenance service provider

service provider that provides support activities for an automation and control solution after handover

Note 1 to entry: Maintenance is often considered to be distinguished from operation (eg.in common colloquial language, it is often assumed that an automation and control solution is either in operation or under maintenance). Maintenance service providers can perform support activities during operations, for example managing user accounts, security monitoring, or security assessments.