

TECHNICAL REPORT

Industrial-process measurement, control and automation – Smart manufacturing – Part 1: Terms and definitions



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2022 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Secretariat
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, ...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch

Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 300 terminological entries in English and French, with equivalent terms in 19 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.



Documents
Document Sharing Hub

TECHNICAL REPORT

**Industrial-process measurement, control and automation – Smart
manufacturing –
Part 1: Terms and definitions**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 25.040.40

ISBN 978-2-8322-1086-0

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

FOREWORD.....	3
INTRODUCTION.....	5
1 Scope.....	6
2 Normative references	6
3 Terms, definitions and abbreviated terms	6
3.1 Terms and definitions.....	6
3.2 Abbreviations	76
Bibliography.....	78

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**INDUSTRIAL-PROCESS MEASUREMENT,
CONTROL AND AUTOMATION –
SMART MANUFACTURING –****Part 1: Terms and definitions****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.

IEC TR 63283-1 has been prepared by IEC technical committee 65: Industrial-process measurement, control and automation. It is a Technical Report.

The text of this Technical Report is based on the following documents:

Draft	Report on voting
65/863/DTR	65/904/RVDTR

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this Technical Report is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/standardsdev/publications.

A list of all parts in the IEC 63283 series, published under the general title *Industrial-process measurement, control and automation – Smart manufacturing*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under 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.

INTRODUCTION

This document presents a vocabulary for terms that can become relevant within the scope of Smart Manufacturing. It is not intended to be a vocabulary for Smart Manufacturing, but it includes more than the terms from the other parts of this series.

INDUSTRIAL-PROCESS MEASUREMENT, CONTROL AND AUTOMATION – SMART MANUFACTURING –

Part 1: Terms and definitions

1 Scope

The scope of this document is to compile a comprehensive collection of base terminology with compatible terms that can become relevant within the scope of Smart Manufacturing. Most of these terms refer to existing definitions in the domain of industrial-process measurement, control and automation and its various subdomains. When multiple similar definitions exist for the exact same term in different standards, this document contains only the preferred definition in the context of Smart Manufacturing. Whenever the existing definitions are not compatible with other terms in this document or when the definition does not fit into the broader scope of Smart Manufacturing, new or modified definitions are given.

2 Normative references

There are no normative references in this document.

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology 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

<X> template

specification of the common features of a collection of <X>s in sufficient detail that an <X> can be instantiated using it in its appropriate context

Note 1 to entry: <X> can be anything that has a type.

[SOURCE: ISO 15745-1:2003, 3.33, modified – "in its appropriate context" added to definition]

3.1.2

access

ability and means to communicate with or otherwise interact with a system in order 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 in to a system and application, through a combination of logical and physical means).

[SOURCE: IEC TS 62443-1-1:2009, 3.2.1]

3.1.3**access control**

protection of system resources against unauthorized access; a process by which 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

[SOURCE: IEC TS 62443-1-1:2009, 3.2.2]

3.1.4**accountability**

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

[SOURCE: IEC TS 62443-1-1:2009, 3.2.3]

3.1.5**action**

something which happens

Note 1 to entry: Every action of interest for modelling purposes is associated with at least one object (see ISO/IEC 10746-2).

[SOURCE: ISO 15745-1:2003, 3.1]

3.1.6**activity**

group of tasks that are classified as having a common objective

[SOURCE: IEC 62264-1:2013, 3.1.1]

3.1.7**actor**

entity that communicates and interacts

Note 1 to entry: These actors can include people, software applications, systems, databases, and even the power system itself.

[SOURCE: IEC 62559-2:2015, 3.2]

3.1.8**actuating drive**

physical unit used for driving mechanically actuated final controlling elements

Note 1 to entry: Examples of actuating drives are electric, hydraulic or pneumatic actuating drives, diaphragm systems or piston actuators.

Note 2 to entry: No actuating drive is required for a final controlling element if the manipulated variable at the controller output is capable of directly influencing the mass flow or energy flow, i.e. without any mechanical intermediate variable quantity.

[SOURCE: IEC 60050-351:2013, 351-56-16]

3.1.9**actuator**

functional unit that receives a signal to drive the final controlling element from its output variable

Note 1 to entry: If the final controlling element is mechanically actuated, it is controlled via an actuating drive. The actuator drives the actuating drive in this case.

[SOURCE: IEC 60050-351:2013, 351-49-07, modified – "generates the manipulated variable" changed to "receives a signal", "of the controlling element", example and figures removed from definition]

3.1.10

adaptive design

interoperability with assistive technology

3.1.11

administrator

user role whose responsibilities include controlling access to and implementing security policies for a system

3.1.12

administration shell

virtual digital and active representation of an Industrie 4.0 component in the Industrie 4.0 system

[SOURCE: IEC PAS 63088:2017, 3.1, modified – "Industrie" added twice, note to entry deleted]

3.1.13

aggregation

<UML> special form of association that specifies a whole-part relationship between the aggregate (whole) and a component part

[SOURCE: ISO 15745-1:2003, 3.3]

3.1.14

alarm

audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a timely response

[SOURCE: IEC 62682:2014, 3.1.7]

3.1.15

algorithm

completely determined finite sequence of instructions by which the values of the output variables may be calculated from the values of the input variables

Note 1 to entry: The behaviour of a system with discrete-value input and output variables (for example a switching system) may be described completely by an algorithm. For a system with continuous-value and continuous-time input and output variables the algorithm is given by or derived from the mathematical relationship between the input and output variables.

[SOURCE: IEC 60050-351:2013, 351-42-27]

3.1.16

allocation

form of coordination control that assigns a resource to an entity

3.1.17

applicable property

data element for the computer-sensible description of a property, a relation or a class

3.1.18

application

<software> software functional element specific to the solution of a problem in industrial-process measurement and control

Note 1 to entry: An application may be distributed among resources, and may communicate with other applications.

[SOURCE: IEC TR 62390:2005, 3.1.2]

3.1.19

application

<general> ordered set of processes, performed by a set of resources, coordinated by a set of interactions intended to accomplish a definite objective

[SOURCE: ISO 18435-1:2009, 3.2]

3.1.20

application programming interface

API

standard set of documented and supported routines that expose operating system programming interfaces and services to applications

Note 1 to entry: An API is usually a source code interface that an operating system, library, or service provides to support requests made by computer programs.

[SOURCE: ISO/IEC TR 13066-2:2016, 2.1, modified – Example deleted]

3.1.21

arbitration

coordination control that determines how a resource should be allocated when there are more requests for the resource than can be accommodated at one time

[SOURCE: IEC 61512-1:1997, 3.2]

3.1.22

architecture

fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution

[SOURCE: IEC PAS 63088:2017, 3.2]

3.1.23

area

physical, geographical or logical grouping of resources determined by the site

EXAMPLE It can contain process cells, production units, production lines, and storage zones.

[SOURCE: IEC 62264-1:2013, 3.1.2]

3.1.24

artificial Intelligence

AI

<engineered system> set of methods or automated entities that together build, optimize and apply a model so that the system can, for a given set of predefined tasks, compute predictions, recommendations, or decisions

Note 1 to entry: AI systems are designed to operate with varying levels of automation.

Note 2 to entry: Predictions can refer to various kinds of data analysis or production (including translating text, creating synthetic images or diagnosing a previous power failure). It does not imply anteriority.

[SOURCE: ISO/IEC 22989:__, 3.1.2]

3.1.25

artificial intelligence

<discipline> study of theories, mechanisms, developments and applications related to artificial intelligence <engineered system> (3.1.24)

[SOURCE: ISO/IEC 22989:__, 3.1.3]

3.1.26

asset

entity owned by or under the custodial duties of an organization, which has either a perceived or actual value to the organization

3.1.27

Asset Administration Shell

AAS

standardized digital representation of an asset

[SOURCE: IEC 63278-1:__, 3.1.2]

3.1.28

association

cooperative relationship between system entities, usually for the purpose of transferring information between them

[SOURCE: IEC TS 62443-1-1:2009, 3.2.7]

3.1.29

assurance

attribute of a system that provides grounds for having confidence that the system operates in such a way that the system security policy is enforced

[SOURCE: IEC TS 62443-1-1:2009, 3.2.8]

3.1.30

attack

assault on a system that derives from an intelligent threat – i.e., an intelligent act that 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 1 to entry: There are different commonly recognized classes of attack:

- a) An "active attack" attempts to alter system resources or affect their operation.
- b) A "passive attack" attempts to learn or make use of information from the system but does not affect system resources.
- c) An "inside attack" is an attack initiated by an entity inside the security perimeter (an "insider") – i.e., an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization.
- d) 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.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.9]

3.1.31

attribute

property or characteristic of an entity

[SOURCE: IEC TR 62390:2005, 3.1.3]

3.1.32**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 necessary changes in controls, policies, or procedures

Note 1 to entry: There are three forms of audit

- a) External audits are conducted by parties who are not employees or contractors of the organization.
- b) Internal audit are conducted by a separate organizational unit dedicated to internal auditing.
- c) Controls self-assessments are conducted by peer members of the process automation function.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.11]

3.1.33**audit log**

traceable record 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.

3.1.34**augmented reality**

accumulation of information, e.g. pictures, from the real world, with additional digital information

3.1.35**authenticate**

verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an information system, or to establish the validity of a transmission

[SOURCE: IEC TS 62443-1-1:2009, 3.2.12]

3.1.36**authentication**

security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information

[SOURCE: IEC TS 62443-1-1:2009, 3.2.13]

3.1.37**authorization**

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

[SOURCE: IEC TS 62443-1-1:2009, 3.2.14]

3.1.38**automated vehicle**

mobile device that includes a control system allowing it to operate either autonomously or under remote control

[SOURCE: IEC TS 62443-1-1:2009, 3.2.15]

3.1.39**automation**

conversion of processes or equipment to automatic operation, or the results of the conversion

[SOURCE: ISO/IEC 2382:2015, 2121284, modified – Note 1 and Note 2 removed]

**Documents**

Document Sharing Hub

3.1.40

automation object

physical or logical entity in the automated system

Note 1 to entry: An example of an automation object is an automation component, a valve or a signal.

[SOURCE: IEC 62714-1:2018, 3.1.2]

3.1.41

autonomous

operating without direct human intervention

3.1.42

availability

ability of an item to be in a state to perform a required function under given conditions at a given instant or over a given time interval, assuming that the required external resources are provided

Note 1 to entry: This ability depends on the combined aspects of the reliability performance, the maintainability performance and the maintenance support performance.

Note 2 to entry: Required external resources, other than maintenance resources do not affect the availability performance of the item.

Note 3 to entry: In French the term "disponibilité" is also used in the sense of "instantaneous availability".

[SOURCE: IEC TS 62443-1-1:2009, 3.2.16, modified – "(performance)" removed]

3.1.43

available capacity

portion of the production capacity that can be attained but is not committed to current or future production

[SOURCE: IEC 62264-1:2013, 3.1.3]

3.1.44

backward compatability

downward compatability

fulfilment by a new component of all the specified requirements of the compatibility profile of its predecessor

[SOURCE: IEC 62890:2020, 3.1.2]

3.1.45

base specification

reference document containing information that is referenced by a profile

[SOURCE: ISO 15745-1:2003, 3.6]

3.1.46

basic control

control that is dedicated to establishing and maintaining a specific state of equipment or process condition

Note 1 to entry: Basic control may include regulatory control, interlocking, monitoring, exception handling, and discrete or sequential control.

[SOURCE: IEC 61512-1:1997, 3.4]

3.1.47**batch**

- (1) material that is being produced or that has been produced by a single execution of a batch process
- (2) entity that represents the production of a material at any point in the process

Note 1 to entry: Batch means both the material made by and during the process and also an entity that represents the production of that material. Batch is used as an abstract contraction of the words "the production of a batch."

[SOURCE: IEC 61512-1:1997, 3.5]

3.1.48**batch control**

control activities and control functions that provide a means to process finite quantities of input materials by subjecting them to an ordered set of processing activities over a finite period of time using one or more pieces of equipment

[SOURCE: IEC 61512-1:1997, 3.6]

3.1.49**batch history**

all execution information collected pertaining to the production of a single batch, and may include common (non-batch specific) information

[SOURCE: IEC 61512-4:2009, 3.1]

3.1.50**batch process**

process that leads to the production of finite quantities of material by subjecting quantities of input materials to an ordered set of processing activities over a finite period of time using one or more pieces of equipment

[SOURCE: IEC 61512-1:1997, 3.7]

3.1.51**batch production**

production process where products or components are produced in batches and where each separate batch consists of a number of the same products or components

[SOURCE: DIN EN 14943:2006-03]

3.1.52**batch production record**

subset of the execution and business information that is retained based upon business requirements identified by the batch production record specification

Note 1 to entry: This information could include the recipe procedural element execution information, both specific equipment information, operator comments, batch-related alarms, elements related to the definition of a batch (such as control recipe, master recipe, site and/or general recipe, batch schedule information), and information important to the batch (such as training logs, maintenance records, and environmental conditions).

[SOURCE: IEC 61512-4:2009, 3.2]

3.1.53**batch schedule**

list of batches to be produced in a specific process cell

Note 1 to entry: The batch schedule typically contains such information as what to produce, how much to produce, when or in what order the batches are needed, and what equipment to use.

[SOURCE: IEC 61512-1:1997, 3.8]

3.1.54
behaviour

observable activities of a component via its effect on its environment and/or through its measurable attributes

[SOURCE: ISO 18435-1:2009, 3.3]

3.1.55
big data

data sets that are too large or complex to be dealt with by traditional data-processing application software

3.1.56
bill of material

listing of all the subassemblies, parts, and/or materials that are used in the production of a product including the quantity of each material required to make a product

Note 1 to entry: The term product can refer to a finished product or an intermediate product.

[SOURCE: IEC 62264-1:2013, 3.1.4]

3.1.57
bill of resources

list of resources needed to produce a product

Note 1 to entry: It is also a listing of the key resources required to manufacture a product, organized as segments of production and is often used to predict the impact of activity changes in the master production schedule on the supply of resources.

Note 2 to entry: The bill of resources does not normally include the consumables.

[SOURCE: IEC 62264-1:2013, 3.1.5]

3.1.58
border

edge or boundary of a physical or logical security zone

[SOURCE: IEC TS 62443-1-1:2009, 3.2.17]

3.1.59
botnet

collection of software robots, or bots, which run autonomously

Note 1 to entry: A botnet's originator can control the group remotely, possibly for nefarious purposes.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.18]

3.1.60
boundary

software, hardware, or other physical barrier that limits access to a system or part of a system

[SOURCE: IEC TS 62443-1-1:2009, 3.2.19]

3.1.61
building block

recipe entity that exists in a library

[SOURCE: IEC 61512-2:2001, 3.2]

3.1.62

business process segment

identification of personnel, equipment, physical assets, and material resources with specific capabilities needed for a segment of production, independent of any particular product at the level of detail required to support business processes that may also be independent of any particular product

Note 1 to entry: The business process segment synonym is included to reflect the business process oriented aspects of the process segment.

[SOURCE: IEC 62264-1:2013, 3.1.26]

3.1.63

capability

ability to perform actions

[SOURCE: IEC 62264-1:2013, 3.1.6]

3.1.64

capability assessment

evaluation of the ability or capacity of a manufacturing asset to provide a resource to the system

[SOURCE: ISO 18435-1:2009, 3.4]

3.1.65

capacity

measure of the ability to take action as an aspect of a capability

EXAMPLE Measures of the production rates, flow rates, mass or volume.

[SOURCE: IEC 62264-1:2013, 3.1.7]

3.1.66

cardinality

pattern defining the number of times a concept reoccurs within a description

[SOURCE: IEC 61360-1:2017, 3.1.3]

3.1.67

cells

lower-level elements that perform manufacturing, field device control, or vehicle functions

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

[SOURCE: IEC TS 62443-1-1:2009, 3.2.68]

3.1.68

channel

specific communication link established within a communication conduit

[SOURCE: IEC TS 62443-1-1:2009, 3.2.20]

3.1.69

characteristic

distinguishing feature

Note 1 to entry: A characteristic can be inherent or assigned.

Note 2 to entry: A characteristic can be qualitative or quantitative.

[SOURCE: IEC 61360-1:2017, 3.1.4]

3.1.70

choreography between services

(self-organizing) interaction between service users in the context of higher-level specifications

[SOURCE: VDI-Statusreport – Industrie 4.0 Begriff / Terms 2019]

3.1.71

ciphertext

data that has been transformed by encryption so that its semantic information content (i.e., its meaning) is no longer intelligible or directly available

[SOURCE: IEC TS 62443-1-1:2009, 3.2.21]

3.1.72

class

<of products> abstraction of a set of similar products

Note 1 to entry: A product that complies with the abstraction defined by a class is called a class member.

Note 2 to entry: A class is an intentional concept that can take different extensional meanings in different contexts.

EXAMPLE The set of products used by a particular enterprise and the set of all ISO-standardized products are two examples of contexts. In these two contexts (the particular enterprise and ISO), the set of products that are considered as members of the single ball bearing class can be different, in particular because employees of each enterprise ignore a number of existing single ball bearing products.

Note 3 to entry: Classes are structured by class inclusion relationships.

Note 4 to entry: A class of products is a general concept as defined in ISO 1087:2019. Thus, it is advisable that the rules defined in ISO 704 be used for defining the designation and definition attributes of classes of products.

Note 5 to entry: In the context of the ISO 13584 series, a class is either a characterization class, associated with properties and usable for characterizing products, or a categorization class, not associated with properties and not usable for characterizing products.

[SOURCE: IEC 61360-1:2017, 3.1.6, modified – "ISO 1087-1" changed to "ISO 1087:2019"]

3.1.73

class

description of a set of objects that share the same specifications of features, constraints, and semantics

[SOURCE: ISO/IEC 19505-1: 2012, 11.4.2, modified – "a class describes" changed to "description of"]

3.1.74

classification

systematic division of a set of items into subsets that share the same specifications of features, constraints, and semantics

3.1.75

classifier

<UML> mechanism that describes behavioural and structural features

Note 1 to entry: Classifiers include interfaces, classes, data types, and components.

[SOURCE: ISO 15745-1:2003, 3.8]

3.1.76

classifying property

property applicable for a particular class, having a value list whose values define the subclasses of the class

[SOURCE: IEC 61360-1:2017, 3.1.7]

3.1.77

client

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

[SOURCE: IEC TS 62443-1-1:2009, 3.2.22]

3.1.78

closed-loop control

process whereby one variable (quantity), namely the controlled variable is continuously measured, compared with another variable (quantity), namely the reference variable, and influenced in such a manner as to adjust the reference variable

Note 1 to entry: Characteristic for closed-loop control is the closed action in which the controlled variable continuously influences itself in the action path of the closed loop.

[SOURCE: IEC 6050-351:2013, 351-47-01, modified – Parenthesis around "quantity" deleted (twice), "or sequentially" deleted from the definition and from the Note to entry]

3.1.79

cloud computing

paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand

Note 1 to entry: Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

[SOURCE: IEC 60050-741:2020, 741-01-07]

3.1.80

cloud service

one or more capabilities offered via *cloud computing* (3.1.79) invoked using a defined interface.

[SOURCE: ISO/IEC 17788:2014, 3.2.8]

3.1.81

committed capacity

portion of the production capacity that is currently in use or is scheduled for use

[SOURCE: IEC 62264-1:2013, 3.1.8]

3.1.82

common resource

resource that can provide services to more than one requester

Note 1 to entry: Common resources are identified as either exclusive-use resources or shared-use resources.

[SOURCE: IEC 61512-1:1997, 3.9]

3.1.83

communication network profile

representation of the integration aspects of a communication network supported by a networked device

EXAMPLE Examples of integration aspects are communication object types and the associated operating relationships (client-server, producer-consumer, etc.), services and attributes for the object types, data types for the object types and services, and encoding rules used.

[SOURCE: ISO 15745-1:2003, 3.9]

3.1.84

communication path

logical connection between a source and one or more destinations, which could be devices, physical processes, data items, commands, or programmatic interfaces

Note 1 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 physical plant, portable mediums, and human interactions.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.23]

3.1.85

communication security

measures that implement and assure security services in a communication system, particularly those that provide data confidentiality and data integrity and that authenticate communicating entities

Note 1 to entry: This phrase is usually understood to include cryptographic algorithms and key management methods and processes, devices that implement them, and the life-cycle management of keying material and devices. However, cryptographic algorithms and key management methods and processes may not be applicable to some control system applications.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.24, modified – item b) deleted]

3.1.86

communication stack

layered set of software modules between the application and the hardware that provides various functions to encode, encrypt and format a message for sending, and to decode, decrypt and unpack a message that was received

[SOURCE: IEC TR 62541-1:2020, 3.1.9]

3.1.87

communication system

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

[SOURCE: IEC TS 62443-1-1:2009, 3.2.25]

3.1.88

compatibility

ability of a new component to satisfy the requirement profile of an original component

[SOURCE: IEC 62890:2020, 3.1.4, modified – circular definition of "compatibility" revised]

3.1.89

compatibility profile

list of all compatibility requirements of a system, or a component of a system, dependent on application specifics

[SOURCE: IEC 62890:2020, 3.1.6]

3.1.90

compliance

relation between two specifications, A and B, that holds when specification A makes requirements which are all fulfilled by specification B (when B complies with A)

[SOURCE: ISO 15745-1:2003, 3.10]

3.1.91

component

entity within a system, which fulfills a defined sub-function

3.1.92

compromise

unauthorized disclosure, modification, substitution, or use of information (including plain text cryptographic keys and other critical security parameters)

[SOURCE: IEC TS 62443-1-1:2009, 3.2.26]

3.1.93

computer-sensible form

specific representation of information allowing processing of the information content by means of a computer

[SOURCE: IEC 61360-1:2017, 3.1.10, modified – changed "an electronic computer" into "a computer"]

3.1.94

concept

unit of knowledge created by a unique combination of characteristics

[SOURCE: IEC 61360-1:2017, 3.1.8]

3.1.95

concept dictionary

collection of entries that allows lookup by concept identifier

Note 1 to entry: There are standardized dictionaries (e.g. IEC CDD), consortium dictionaries (e.g. eOTD®¹ and ECLASS®²), supplier dictionaries and DF dictionaries.

[SOURCE: IEC 62832-1:2020, 3.1.5, modified – "concept dictionary" deleted in the definition]

3.1.96

concept dictionary entry

definition of a concept containing, at a minimum, an unambiguous concept identifier, a preferred name, and a description

[SOURCE: IEC 62832-1:2020, 3.1.6]

¹ eOTD® is the registered trademark of a product supplied by ECCMA (Electronic Commerce Code Management Association). This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the product named.

² ECLASS® is the registered trademark of a product supplied by the ECLASS e.V. association. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the product named.

3.1.97

conduit

logical grouping of communication assets that protects the security of the channels it contains

Note 1 to entry: This is analogous to the way that a physical conduit protects cables from physical damage.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.27]

3.1.98

confidentiality

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

[SOURCE: IEC TS 62443-1-1:2009, 3.2.28]

3.1.99

configuration

<of a system or device> selecting functional units, assigning their locations and defining their interconnections

[SOURCE: IEC 61804-2:2018, 3.1.12]

3.1.100

consumables

resources that are not individually accounted for in specific production requests, not normally included in bills of material, or not lot tracked

[SOURCE: IEC 62264-1:2013, 3.1.9]

3.1.101

continuous production

production that is running at a steady rate

[SOURCE: ISO 2859-3:2005, 3.1.1, modified – "running" added and Note deleted]

3.1.102

control application

type of (manufacturing) application that monitors availability, identifies the conditions of manufacturing assets and provides other applications with such information in order to accomplish a manufacturing production objective

[SOURCE: ISO 18435-1:2009, 3.6, modified – Introduced the parentheses around "manufacturing" and replaced the "and" after "availability" with a comma]

3.1.103

control center

central location used to operate a set of assets

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 (for example, a backup center at a separate site), they are typically connected together via a wide area network. The control center contains the SCADA system, host computers and associated operator display devices plus ancillary information systems such as an historian.

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

[SOURCE: IEC TS 62443-1-1:2009, 3.2.29]

3.1.104**control equipment**

class that includes distributed control systems, programmable logic controllers, SCADA systems, associated operator interface consoles, field sensing and final control equipment used to manage and control the process

[SOURCE: IEC TS 62443-1-1:2009, 3.2.30, modified – Note deleted, "control devices" changed to "final control equipment"]

3.1.105**control module**

lowest level grouping of equipment in the physical model that can carry out basic control

Note 1 to entry: This term applies to both the physical equipment and the equipment entity.

[SOURCE: IEC 61512-1:1997, 3.10]

3.1.106**control network**

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

Note 1 to entry: The control network can be subdivided into zones and there can be multiple separate control networks within one company or site.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.31]

3.1.107**control recipe**

type of recipe which, through its execution, defines the manufacture of a single batch of a specific product

[SOURCE: IEC 61512-1:1997, 3.11]

3.1.108**coordination control**

type of control that directs, initiates, and/or modifies the execution of procedural control and the utilization of equipment entities

[SOURCE: IEC 61512-1:1997, 3.12]

3.1.109**core model**

reference model of basic concepts and contexts which concern a general aspect of systems

[SOURCE: VDI-Statusreport – Industrie 4.0 Begriff / Terms 2019]

3.1.110**corrective maintenance**

maintenance carried out after fault detection to effect restoration

[SOURCE: IEC 60050-192:2015, 192-06-06, modified – Note 1 to entry deleted]

3.1.111**cost**

value of impact to an organization or person that can be measured

[SOURCE: IEC TS 62443-1-1:2009, 3.2.32]

3.1.112**countermeasure**

action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken

Note 1 to entry: The term "control" is also used to describe this concept in some contexts. The term countermeasure has been chosen for this document to avoid confusion with the term "control" in the context of process control.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.33]

3.1.113**cryptographic algorithm**

well-defined computational procedure that takes variable inputs, which may include cryptographic keys, and produces an output

[SOURCE: ISO/IEC 19790:2012, 3.20]

3.1.114**cryptographic key**

input parameter that varies the transformation performed by a cryptographic algorithm

Note 1 to entry: Usually shortened to "key".

[SOURCE: IEC TS 62443-1-1:2009, 3.2.35]

3.1.115**cyber-physical production system****CPPS**

CPS which is used in production

[SOURCE: VDI-Statusreport – Industrie 4.0 Begriff / Terms 2019]

3.1.116**cyber-physical system****CPS**

system which links real (physical) objects and processes with information-processing (virtual) objects and processes via open, in some cases global, and constantly interconnected information networks

Note 1 to entry: A CPS optionally uses services available locally or remotely, has human-machine interfaces, and offers the possibility of dynamic adaptation of the system at runtime.

[SOURCE: VDI-Statusreport – Industrie 4.0 Begriff / Terms 2019]

3.1.117**cybersecurity**

actions required to preclude unauthorized use of, denial of service to, modifications to, disclosure of, loss of revenue from, or destruction of critical systems or informational assets

Note 1 to entry: The objective is to reduce the risk of causing personal injury or endangering public health, losing public or consumer confidence, disclosing sensitive assets, failing to protect business assets or failing to comply with regulations. These concepts are applied to any system in the production process and include both stand-alone and networked components. Communications between 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 control systems. Cybersecurity includes the concepts of identification, authentication, accountability, authorization, availability, and privacy.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.36]

3.1.118**data**

reinterpretable representation of information in a formalized manner suitable for communication, interpretation or processing

[SOURCE: IEC TR 62390:2005, 3.1.5]

3.1.119**data compatibility**

fulfilment of requirements from a functional view of a compatibility profile related to the specific data type and data format by a component

[SOURCE: IEC 62890:2020, 3.1.9, modified – "functional aspects related to data type and format of a compatibility profile" changed to "requirements from a functional view of a compatibility profile related to the specific data type and data format"]

3.1.120**data confidentiality**

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

[SOURCE: IEC TS 62443-1-1:2009, 3.2.37]

3.1.121**data connection**

association established between functional units for conveyance of data

[SOURCE: IEC 61804-2:2018, 3.1.14]

3.1.122**data element**

pair consisting of the identifier of a data element type and a corresponding value

3.1.123**data element relationship**

relationship between data element types or between data elements in a given context

[SOURCE: IEC 62832-1:2020, 3.1.8]

3.1.124**data element type**

unit of data for which the identification, description and permissible values have been specified according to a data specification

[SOURCE: IEC 62832-1:2020, 3.1.9]

3.1.125**data historian**

capability of a system to permanently collect operating information of that system

[SOURCE: ISO 18435-1:2009, 3.8, modified – "permanently" added to the definition]

3.1.126**data integrity**

property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner

Note 1 to entry: This term deals with constancy of and confidence in data values, not with the information that the values represent or the trustworthiness of the source of the values.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.38]

3.1.127

data specification

rules for describing items belonging to a particular class using entries from a concept dictionary and reference to a specific formal syntax

EXAMPLE An ISO/TS 22745-30 compliant identification guide, ISO 13584-511 are data specifications.

[SOURCE: IEC 62832-1:2020, 3.1.10, modified – ISO 8000-2 removed from the example]

3.1.128

data type

set of values together with a set of permitted operations

[SOURCE: IEC 61804-2:2018, 3.1.17]

3.1.129

data quality

degree to which a set of inherent characteristics of data fulfils requirements

Note 1 to entry: The principles of data quality involves:

- data being fit for purpose; i.e., the decision in which the data is used;
- having the right data, in the right place, at the right time;
- meeting agreed customer requirements for the data;
- preventing the recurrence of data defects by improving processes to prevent repetition and eliminate wasted effort.

[SOURCE: ISO 8000-2:2020, 3.8.1, modified – Note 1 to entry changed]

3.1.130

decryption

process of changing cipher text into plain text using a cryptographic algorithm and key

[SOURCE: IEC TS 62443-1-1:2009, 3.2.39]

3.1.131

defence in depth

provision of multiple security protections, especially in layers, with the intent to delay if not prevent an attack

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

- 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;
- a system security becomes a set of layers within the overall network security.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.40]

3.1.132

delivery release

end of the manufacturing preparation process after which series production can begin

[SOURCE: IEC 62890:2020, 3.1.10, modified – Note 1 to entry deleted]