

TECHNICAL REPORT

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

IECNORM.COM : Click to view the full PDF of IEC TR 63283-1:2022



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 It also gives information on projects, replaced and withdrawn publications.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.

IECNORM.COM : Click to view the full PDF of IEC 60328-1:2022

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

IECNORM.COM : Click to view the full PDF of IEC TR 63283-1:2022

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.

IECNORM.COM : Click to view the full PDF of IEC TR 63283-1:2022

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.

IECNORM.COM : Click to view the full PDF of IEC TR 63283-1:2022

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]

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]

3.1.133**demilitarized zone**

perimeter network segment that is logically inserted between internal and external networks

Note 1 to entry: The purpose of a demilitarized zone 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 industrial 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.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.41]

3.1.134**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 industrial automation and control systems, denial of service can refer to loss of process function, not just loss of data communications.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.42]

3.1.135**detailed production schedule**

organized and structured collection of production work orders and sequencing involved in the production of one or more products

3.1.136**development phase**

phase of the product life cycle which begins with the decision to develop a product type and ends with delivery release of the product type

[SOURCE: IEC 62890:2020, 3.1.11]

3.1.137**device**

independent physical entity capable of performing one or more specified functions in a particular context and delimited by its interfaces

[SOURCE: IEC 61804-2:2018, 3.1.18]

3.1.138**device management application**

application whose primary function is the management of multiple resources within a device

[SOURCE: IEC 61804-2:2018, 3.1.20]

3.1.139**device profile**

representation of a device in terms of its parameters, parameter assemblies and behaviour according to a device model that describes the data and behaviour of the device as viewed through a network, independent from any network technology

Note 1 to entry: The mapping onto a given network technology is the task of the communication profile.

[SOURCE: IEC TR 62390:2005, 3.1.9, modified – Note 1 removed, Note 2 changed to Note 1]

3.1.140

field device

device that performs control, actuating and/or sensing functions

3.1.141

diagnostics application

type of (manufacturing) application that monitors and checks the continued availability of manufacturing assets, and notifies the other (manufacturing) applications of any conditions or constraints on such availability

[SOURCE: ISO 18435-1:2009, 3.7, modified – Introduced the parentheses around "manufacturing"]

3.1.142

Digital Factory

digital representation of a production system

Note 1 to entry: A Digital Factory can represent an existing or planned production system.

Note 2 to entry: The representation of a production system can include representation of PS assets and representation of roles.

[SOURCE: IEC 62832-1:2020, 3.1.19]

3.1.143

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

[SOURCE: IEC TS 62443-1-1:2009, 3.2.43]

3.1.144

direct influence

environmental influence resulting from actual product production by direct operation of manufacturing equipment

[SOURCE: IEC TR 62837:2013, 3.7.1]

3.1.145

discrete manufacturing

method of manufacturing where products are manufactured in a non-continuous manner, e.g. automobiles, appliances, computers

[SOURCE: DIN EN 14943:2006-03]

3.1.146

disposal

recycling or removal of a product instance following the time in use, as the last phase of the life time, with respect to regulations

[SOURCE: IEC 62890:2020, 3.1.12, modified – "and disposal or recycling" replaced by "as the last phase of the life time, with respect to regulations"]

3.1.147

distributed control system

DCS

type of control system in which the system elements are dispersed but operated in a coupled manner

Note 1 to entry: Distributed control systems may have shorter coupling time constants than those typically found in SCADA systems.

Note 2 to entry: Distributed control systems are commonly associated with continuous processes such as electric power generation, oil and gas refining, chemical, pharmaceutical and paper manufacture, as well as discrete processes such as automobile and other goods manufacture, packaging, and warehousing.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.44]

3.1.148

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

[SOURCE: IEC TS 62443-1-1:2009, 3.2.45]

3.1.149

dynamic testing

executing software and/or operating hardware in a controlled and systematic way, so as to demonstrate the presence of the required behaviour and the absence of unwanted behavior

3.1.150

eavesdropping

monitoring or recording of communicated information by unauthorized parties

[SOURCE: IEC TS 62443-1-1:2009, 3.2.46]

3.1.151

electronic device description

EDD

data collection containing the device parameter(s), their dependencies, their graphical representation and a description of the data sets which are transferred

Note 1 to entry: The electronic device description is created using the electronic device description language (EDDL).

[SOURCE: IEC 61804-2:2018, 3.1.25]

3.1.152

edge

boundary between pertinent digital and physical entities, delineated by networked sensors and actuators

[SOURCE: ISO/IEC TR 30164:2020, 3.1]

3.1.153

edge computing

distributed computing that takes place at or near the edge, where the nearness is defined by the system's requirements

[SOURCE: ISO/IEC TR 30164:2020, 3.2]

3.1.154

electronic device description language

EDDL

methodology for describing parameter(s) of an automation system component

[SOURCE: IEC 61804-2:2018, 3.1.24]

3.1.155

embedded systems

devices with built-in microprocessors for signal processing for predetermined tasks

3.1.156

encryption

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

Note 1 to entry: If the transformation is reversible, the corresponding reversal process is called "decryption," which is a transformation that restores encrypted data to its original state.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.47]

3.1.157

end of product sales

discontinuation of a product

end of all active sales activities for a product

[SOURCE: IEC 62890:2020, 3.1.13, modified – Note to entry removed, "discontinuation of a product" added as synonym, "product" added to the term]

3.1.158

end of production

point of time when instances of a product type are no longer produced

[SOURCE: IEC 62890:2020, 3.1.15]

3.1.159

end of service

end of all service activities for a product type

[SOURCE: IEC 62890:2020, 3.1.14]

3.1.160

energy baseline

quantitative reference(s) providing a basis for comparison of energy performance

Note 1 to entry: An energy baseline reflects a specified period of time.

Note 2 to entry: An energy baseline can be normalized using variables affecting energy use and/or consumption such as production level, degree days (outdoor temperature), etc.

Note 3 to entry: Energy baseline is also used for calculation of energy savings, as a reference before and after implementation of energy performance improvement actions.

[SOURCE: IEC TR 62837:2013, 3.2.1]

3.1.161

energy demand

necessary supply capacity for the projected level of energy use

Note 1 to entry: When considering future trends, energy demand is often used in the sense of potential energy consumption.

Note 2 to entry: Energy demand is often used in the context of supply-demand interaction where demand is not given but dependent on external factors such as energy prices.

[SOURCE: IEC TR 62837:2013, 3.2.3]

3.1.162**energy efficiency**

ratio between an output of performance, service, goods or energy, and an input of energy

Note 1 to entry: Both input and output have to be clearly specified in quantity and quality, and be measurable.

Note 2 to entry: Examples are conversion efficiency, energy required/energy used, output/input, theoretical energy used to operate/energy used to operate.

[SOURCE: IEC TR 62837:2013, 3.3.1]

3.1.163**energy managed unit****EMU**

unit of asset for energy management, identified by an energy related functional partitioning

[SOURCE: IEC TR 62837:2013, 3.5.3]

3.1.164**energy performance**

measurable results related to energy efficiency, energy use and energy consumption

Note 1 to entry: In the context of energy management systems, results can be measured against the organization's energy policy, objectives, targets and other energy performance requirements.

Note 2 to entry: Energy performance is one component of the performance of the energy management system.

[SOURCE: IEC TR 62837:2013, 3.4.1]

3.1.165**energy performance indicator****EnPI**

quantitative value or measure of energy performance as defined by the organization

Note 1 to entry: EnPIs could be expressed as a simple metric, ratio or a more complex model.

[SOURCE: IEC TR 62837:2013, 3.4.2]

3.1.166**energy saving**

reduction of energy consumption following implementation of energy efficiency improvement action(s)

Note 1 to entry: The reduction is obtained by comparison against the baseline taking into account all adjustment factors.

Note 2 to entry: Energy savings can be potential following an assessment or actual after implementing an action(s).

[SOURCE: IEC TR 62837:2013, 3.2.5]

3.1.167**enterprise**

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

[SOURCE: IEC 62264-1:2013, 3.1.10]

3.1.168

enterprise 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)

[SOURCE: IEC TS 62443-1-1:2009, 3.2.49]

3.1.169

entity

thing (physical or non-physical) having a distinct existence

[SOURCE: ISO/IEC 20924:2021, 3.1.18]

3.1.170

equipment

one or more entities that perform a certain function

3.1.171

Ethernet

a carrier sense, multiple access collision detect (CSMA/CD) local area network protocol standard as defined in IEEE 802.3 and later revisions and additions to IEEE 802

[SOURCE: IEC 61162-450:2018, 3.6, modified – Note 1 to entry deleted]

3.1.172

exception

event that causes suspension of normal execution

[SOURCE: IEC 61804-2:2018, 3.1.32]

3.1.173

exception handling

functions that deal with plant or process contingencies and other events which occur outside the normal or desired behaviour of batch control

[SOURCE: IEC 61512-1:1997, 3.21]

3.1.174

exchange table

database table that is used to exchange batch-related information between systems

[SOURCE: IEC 61512-2:2001, 3.4]

3.1.175

exclusive-use resource

common resource that only one user can use at any given time

[SOURCE: IEC 61512-1:1997, 3.22]

3.1.176

execution

process of carrying out a sequence of operations specified by an algorithm

[SOURCE: IEC TR 62390:2005, 3.1.11]

3.1.177**feature**

aspect of an item that can be captured by a class structure and set of properties and that cannot exist independently of the item

[SOURCE: IEC 61360-1:2017, 3.1.14]

3.1.178**field I/O network**

communication links (wired or wireless) that connects sensors and actuators to the control equipment

[SOURCE: IEC TS 62443-1-1:2009, 3.2.51]

3.1.179**final controlling element**

functional unit forming part of the controlled system and arranged at its input, driven by the manipulated variable and manipulating the mass flow or energy flow

Note 1 to entry: If the final controlling element is mechanically actuated, an additional actuator (positioner) is used in some cases.

Note 2 to entry: The output variable of the final controlling equipment is usually not free from feedback. The interface between the actuator and the final controlling element should therefore be selected in such a way that the manipulated variable is not affected by feedback from the final controlling element.

Note 3 to entry: Variable frequency drives (VFD) are also frequently used as final control elements.

[SOURCE: IEC 60050-351:2013, 351-49-08, modified – Figures deleted and Note 3 to entry modified]

3.1.180**final controlling equipment**

functional unit that consists of an actuator and a final controlling element

[SOURCE: IEC 60050-351:2013, 351-49-09, modified – Figures and Note 1 to entry deleted]

3.1.181**finished goods**

final materials on which all processing and production is completed

[SOURCE: IEC 62264-1:2013, 3.1.12]

3.1.182**finished goods waiver**

approval for deviation from normal product specifications

[SOURCE: IEC 62264-1:2013, 3.1.13]

3.1.183**finite capacity scheduling**

scheduling methodology where work is scheduled for production equipment, in such a way that no production equipment capacity requirement exceeds the capacity available to the production equipment

[SOURCE: IEC 62264-3:2016, 3.1.1]

3.1.184

firewall

inter-network connection device that restricts data communication traffic between two connected networks

[SOURCE: IEC TS 62443-1-1:2009, 3.2.52, modified – Note deleted]

3.1.185

formula

category of recipe information that includes process inputs, process parameters and process outputs

[SOURCE: IEC 61512-1:1997, 3.23]

3.1.186

full compatibility

fulfillment of all requirements of the compatibility profile from the function, construction, location, and performance view by a component

3.1.187

function

intended purpose of an entity or its characteristic action

[SOURCE: IEC 61804-2:2018, 3.1.33]

3.1.188

functional requirement

specification of a behaviour that a solution or part of a solution shall perform

3.1.189

function block

function block instance

software functional unit comprising an single, named copy of a data structure and associated operations specified by a corresponding FB type

Note 1 to entry: Typical operations of a FB include modification of the values of the data in its associated data structure.

[SOURCE: IEC 61804-2:2018, 3.1.35, modified – "individual" changed to "single"]

3.1.190

function chart

graphic description tool with symbolic representation of sequential control systems

Note 1 to entry: The symbolic representation of steps, commands, transitions and directed links is based on input and output Boolean variables and also on internal state variables and binary delay elements.

Note 2 to entry: The elements, rules and basic structures for function charts are given in IEC 60848.

[SOURCE: IEC 60050-351:2013, 351-53-08, modified – Word "tool" added in the definition and Note 2 to entry slightly shortened]

3.1.191

function compatibility

fulfilment of all requirements of the compatibility profile from the functional view by a component

[SOURCE: IEC 62890:2020, 3.1.17, modified – "functional aspects of a compatibility profile" changed to "all requirements of the compatibility profile", and "from the functional view" added]

3.1.192**functional element**

entity of software or software combined with hardware, capable of accomplishing a specified function of a device

Note 1 to entry: A functional element has an interface, associations to other functional elements and functions.

Note 2 to entry: A functional element can be made out of function block(s), object(s) or parameter list(s).

[SOURCE: IEC TR 62390:2005, 3.1.12]

3.1.193**functional safety**

part of the overall safety that depends on functional and physical units operating correctly in response to their inputs

[SOURCE: IEC 60050-351: 351-57-06, modified – Note 1 to entry deleted]

3.1.194**functional unit**

entity of hardware or software, or both, capable of accomplishing a specified purpose

[SOURCE: IEC 61804-2:2018, 3.1.34]

3.1.195**gateway**

network component that acts as a linking element between different communication network types and/or protocols

Note 1 to entry: In OSI-conforming communication networks, a gateway operates on Layer 4 up to layer 7. It allows networks based on completely different protocols to communicate with each other and possibly provides additional functionality.

3.1.196**general recipe**

type of recipe that expresses equipment and site-independent processing requirements

[SOURCE: IEC 61512-1:1997, 3.24]

3.1.197**generalization**

<UML> taxonomic relationship between a more general element and a more specific element

Note 1 to entry: The more specific element is fully consistent with the more general element and contains additional information. An instance of the more specific element may be used where the more general element is allowed.

[SOURCE: ISO 15745-1:2003, 3.17]

3.1.198**geographic site**

subset of an enterprise's physical, geographic, or logical group of assets

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

[SOURCE: IEC TS 62443-1-1:2009, 3.2.54]

3.1.199

guard

gateway that is interposed between two networks (or computers or other information systems) operating at different security levels (one network is usually more secure than the other) and is trusted to mediate all information transfers between the two networks, either to ensure that no sensitive information from the more secure network is disclosed to the less secure network, or to protect the integrity of data on the more secure network

[SOURCE: IEC TS 62443-1-1:2009, 3.2.55]

3.1.200

hardware

physical equipment, as opposed to programs, procedures, rules and associated documentation

[SOURCE: IEC 61804-2:2018, 3.1.37]

3.1.201

harm

injury or damage to the health of people, or damage to property or the environment

[SOURCE: ISO/IEC GUIDE 51:2014, 3.1]

3.1.202

hazard

potential source of harm

[SOURCE: ISO/IEC GUIDE 51:2014, 3.2]

3.1.203

hazardous event

event that can cause harm

[SOURCE: ISO/IEC GUIDE 51:2014, 3.3]

3.1.204

header

information about the purpose, source and version of the recipe such as recipe and product identification, creator, and issue date.

[SOURCE: IEC 61512-1:1997, 3.25]

3.1.205

horizontal integration

integration within a functional/organizational hierarchical level across system boundaries

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

3.1.206

host

computer that is attached to a communication sub-network or inter-network and can use services provided by the network to exchange data with other attached systems

[SOURCE: IEC TS 62443-1-1:2009, 3.2.56]

3.1.207

human profile

representation of the integration aspects of a person

EXAMPLES: Examples of integration aspects are level of responsibility, level of competency, availability.

[SOURCE: ISO 15745-1:2003, 3.18]

3.1.208
identifier
ID

information that unambiguously distinguishes one entity from other entities in a given identity context

[SOURCE: IEC 60050-741: 2020, 741-01-21]

3.1.209
impact

evaluated consequence of a particular event

Note 1 to entry: Impact may be expressed in terms of numbers of injuries and/or fatalities, extent of environmental damage and/or magnitude of losses such as property damage, material loss, loss of intellectual property, lost production, market share loss, and recovery costs.

3.1.210
implementation phase

development phase in which the hardware and software of a system become operational

[SOURCE: IEC 61804-2:2018, 3.1.38, modified – added "implementation" to the term defined]

3.1.211
incident

event that is not part of the expected operation of a system or service that causes, or may cause, an interruption to, or a reduction in, the quality of the service provided by the control system

3.1.212
intelligent features

characteristics, such as deduction and analysis, in addition to those needed to achieve scheduled functions and tasks

EXAMPLE For example, as to intelligent products, identified aspects of intelligent features with and devices include perception and sensing, interconnection, diagnosis and maintenance, adaptive optimization, information services, interactive cooperation, artificial intelligence.

3.1.213
independent equipment

equipment that possesses both of the following characteristics:

- 1) the ability to perform its required function is unaffected by the operation or failure of other equipment;
- 2) the ability to perform its function is unaffected by the occurrence of the effects resulting from the postulated initiating event for which it is required to function

Note 1 to entry: Means to achieve independence in the design are electrical isolation, physical separation and communications independence.

[SOURCE: IEC 61513:2011, 3.31]

3.1.214
industrial automation and control systems
IACS

collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process

Note 1 to entry: These systems include, but are not limited to:

- industrial control systems, including distributed control systems (DCSs), programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices, supervisory control and data acquisition (SCADA), networked electronic sensing and control, and monitoring and diagnostic systems. (In this context, process control systems include basic process control system and safety-instrumented system (SIS) functions, whether they are physically separate or integrated.)
- associated information systems such as advanced or multivariable control, online optimizers, dedicated equipment monitors, graphical interfaces, process historians, manufacturing execution systems, and plant information management systems.
- associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.57]

3.1.215

information

structured data that are endowed with meaning and purpose

Note 1 to entry: Information is data that have been shaped into a form that is meaningful and useful to human beings.

[SOURCE: IEC 60050-741: 2020, 741-01-500]

3.1.216

information model

formal model of a bounded set of facts, concepts or instructions to meet a specified requirement

3.1.217

information object

well-defined piece of information, definition, or specification which requires a name in order to identify its use in communication

[SOURCE: IEC 61360-1:2017, 3.1.15]

3.1.218

information world

digital world

cyber world

ideas, concepts, algorithms, models and entirety of representations of physical objects and people in the virtual environment

Note 1 to entry: The framework for considering each entirety needs to be defined.

Note 2 to entry: The elements of the information world can be semantically related to each other.

Note 3 to entry: Consider information world, cyber world, virtual world and digital world to be synonymus

[SOURCE: IEC PAS 63088:2017, 3.7, modified – Note 3 to entry added]

3.1.219

inherently safe design

measures taken to eliminate hazards and/or to reduce risks by changing the design or operating characteristics of the product or system

[SOURCE: ISO/IEC GUIDE 51:2014, 3.5]

3.1.220

initial risk

risk before controls or countermeasures have been applied

[SOURCE: IEC TS 62443-1-1:2009, 3.2.58]

3.1.221**input**

product, material or energy flow that enters a unit process

[SOURCE: IEC TR 62837:2013, 3.7.3]

3.1.222**input data**

data transferred from an external source into a device, resource or functional element

[SOURCE: IEC TR 62390:2005, 3.1.14]

3.1.223**input variable**

variable whose value is supplied by a data input, and which may be used in one or more operations of a FB

Note 1 to entry: An input parameter of a FB, as defined in IEC 61131-3, is an input variable.

[SOURCE: IEC 61804-2:2018, 3.1.40]

3.1.224**insider**

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

[SOURCE: IEC TS 62443-1-1:2009, 3.2.59]

3.1.225**instance**

concrete, clearly identifiable entity of a certain type

3.1.226**instance**

<software> functional element comprising an individual, named copy of a data structure and associated operations specified by a corresponding functional element type

[SOURCE: IEC TR 62390:2005, 3.1.15]

3.1.227**instance name**

identifier associated with and designating an instance

[SOURCE: IEC 61804-2:2018, 3.1.42]

3.1.228**instantiation**

creation of an instance of a specified type

[SOURCE: IEC 61804-2:2018, 3.1.43]

3.1.229**integration**

process of assembling software and/or hardware items, according to the architectural and design specification, and testing the integrated unit

3.1.230

integrity

quality of a system reflecting the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data

Note 1 to entry: In a formal security mode, integrity is often interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.60]

3.1.231

intended use

use in accordance with information provided with a product or system, or, in the absence of such information, by generally understood patterns of usage

[SOURCE: ISO/IEC GUIDE 51:2014, 3.6]

3.1.232

interaction

transaction involving multiple resources to accomplish some part of a system's function

EXAMPLE Examples include coordination, collaboration, cooperation, unwitting assistance, witting non-interference, and even competition.

[SOURCE: ISO 18435-1:2009, 3.10]

3.1.233

interception

sniffing

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

[SOURCE: IEC TS 62443-1-1:2009, 3.2.61]

3.1.234

interface

shared boundary between two entities defined by functional characteristics, signal characteristics, or other characteristics as appropriate

[SOURCE: IEC 61800-7-1: 2015, 3.2.15]

3.1.235

intermediate database

intermediate data storage system between source and target tool

[SOURCE: IEC 62424:2016, 3.19]

3.1.236

internal variable

variable whose value is used or modified by one or more operations of a FB but is not supplied by a data input or to a data output

[SOURCE: IEC 61804-2:2018, 3.1.47]

3.1.237**Internet of Things****IoT**

infrastructure of interconnected entities, people, systems and information resources together with services which processes and reacts to information from the physical world and virtual world

[SOURCE: ISO/IEC 20924:2021, 3.2.4]

3.1.238**Industrial Internet of Things****IIoT**

service driven industrial ecosystem based on the network interconnection, data interoperability and system interoperability of industrial resources, to realize the flexible configuration of the manufacturing of materials, the on-demand execution of the manufacturing process, the rational optimization of the manufacturing process and the rapid adaptation of the manufacturing environment, and to achieve the efficient utilization of the resources

3.1.239**interoperability**

capability of two or more entities to exchange items in accordance with a set of rules and mechanisms implemented by an interface in each entity, in order to perform their respective tasks

Note 1 to entry: Examples of entities include devices, equipment, machines, people, processes, applications, software units, systems and enterprises.

Note 2 to entry: Examples of items include information, material, energy, control, assets and ideas.

[SOURCE: ISO 18435-1:2009, 3.12]

3.1.240**intrusion**

unauthorized act of compromising a system

[SOURCE: IEC TS 62443-1-1:2009, 3.2.63]

3.1.241**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

[SOURCE: IEC TS 62443-1-1:2009, 3.2.64]

3.1.242**invocation**

process of initiating the execution of the sequence of operations specified in an algorithm

[SOURCE: IEC 61804-2:2018, 3.1.50]

3.1.243**IP address**

address of a host computer used in the Internet Protocol

[SOURCE: IEC 60050-732:2010, 732-07-06, modified – Notes deleted]

3.1.244

job list

production dispatch list

collection of job orders for one or more work centers and/or resources for a specific time frame

Note 1 to entry: This may take the form of job orders for the set-up instructions for machines, operating conditions for continuous processes, material movement instructions, or batches to be started in a batch system.

Note 1 to entry: Job lists are applicable to all operations management areas, such as maintenance, quality test and inventory.

[SOURCE: IEC 62264-3:2016, 3.1.3, modified – "production dispatch list" added as synonym]

3.1.245

job order

production work order

unit of scheduled work that is dispatched for execution

[SOURCE: IEC 62264-4:2015, 3.1.3, modified – "production work order" added as synonym]

3.1.246

job response

information on the result of execution of a job order

[SOURCE: IEC 62264-4:2015, 3.1.4]

3.1.247

job response list

collection of job responses for one or more work centers and/or resources for a specific time frame

[SOURCE: IEC 62264-4:2015, 3.1.5]

3.1.248

key management

process of handling and controlling cryptographic keys and related material (such as initialization values) during their life cycle in a cryptographic system, including ordering, generating, distributing, storing, loading, escrowing, archiving, auditing, and destroying the keys and related material

[SOURCE: IEC TS 62443-1-1:2009, 3.2.67]

3.1.249

key performance indicator

KPI

quantifiable level of achieving a critical objective

Note 1 to entry: The KPIs are derived directly from, or through an aggregation function of, physical measurements, data and/or other KPIs.

[SOURCE: ISO 22400-1:2014, 2.1.5]

3.1.250

last-time buy

strategy in which instances of an abandoned product type are purchased before end of sales

[SOURCE: IEC 62890:2020, 3.1.19]

3.1.251**level of compatibility**

degree of fulfillment of the requirements described in the compatibility profile

[SOURCE: IEC 62890:2020, 3.1.20, modified – added "degree of"]

3.1.252**life cycle**

set of distinguishable phases and steps within phases that an entity goes through from its creation until it ceases to exist

[SOURCE: IEC TR 63319:__, 3.1.2]

3.1.253**life time**

length of time from the end of the creation of a product instance to the end of disposal

[SOURCE: IEC 62890:2020, 3.1.21]

3.1.254**life-cycle excellence**

holistic approach to managing changing conditions to ensure technical, application specific and economic robustness of the life-cycle management for products (components and systems)

[SOURCE: IEC 62890:2020, 3.1.24, modified – Added "(components and systems)"]

3.1.255**life-cycle management**

methods and activities for the planning, realization and maintenance of products for the life cycle of types and the life time of instances

[SOURCE: IEC 62890:2020, 3.1.25]

3.1.256**life-cycle management strategy**

strategy for applying life cycle management methods to ensure the availability of a system throughout the time in use

[SOURCE: IEC 62890:2020, 3.1.26]

3.1.257**limiting value**

greatest or smallest admissible value of a quantity in a specification of a component, device, equipment, or system beyond which it will be damaged resulting in permanent unwanted changes of functional or physical characteristics influencing its performance

[SOURCE: IEC 61360-1:2017, 3.1.17, modified – "beyond which it incurs damage" replaced by beyond which it will be damaged"]

3.1.258**link**

object that specifies the connection between two other objects (for example, the connection between recipe entities or between recipe entities and transitions)

[SOURCE: IEC 61512-2:2001, 3.5]

3.1.259

load shedding

process of deliberately disconnecting preselected loads from a power system in response to an abnormal condition in order to maintain the integrity of the remainder of the system

[SOURCE: IEC TR 62837:2013, 3.3.6]

3.1.260

local area network

LAN

computer network located on a user's premises within a limited geographical area

Note 1 to entry: Communication within a local area network is not subject to external regulations; however, communication across the network boundary may be subject to some form of regulation.

[SOURCE: IEC 60050-732:2010, 732-01-04]

3.1.261

location

scope of exchanged information as identified by an element of the equipment hierarchy

EXAMPLE: There can be an agreement to only supply an "Area" name for exchanged information, because the site and enterprise are implicitly defined through the messaging system

[SOURCE: IEC 62264-2:2013, 3.1.3]

3.1.262

lot

unique amount of material having a set of common traits

Note 1 to entry: Some examples of common traits are material source, the master recipe used to produce the material and distinct physical properties.

[SOURCE: IEC 61512-1:1997, 3.28]

3.1.263

lot size one

small quantity ('one') of goods ordered for delivery on a specific date or manufactured in a single production run

3.1.264

lines, units, 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]

3.1.265

Machine to Machine

M2M

exchange of information between networked devices without the manual assistance of humans

3.1.266**maintenance application**

type of manufacturing application that manages the reconfiguration, removal, replacement or repair of the manufacturing assets, and notifies the other manufacturing applications of such activities

[SOURCE: ISO 18435-1:2009, 3.13]

3.1.267**malicious code**

programs or code written for the purpose of gathering information about systems or users, destroying system data, providing a foothold for further intrusion into a system, falsifying system data and reports, or providing time-consuming irritation to system operations and maintenance personnel

Note 1 to entry: Malicious code attacks can take the form of viruses, worms, Trojan horses, or other automated exploits.

Note 2 to entry: Malicious code is also often referred to as "malware".

[SOURCE: IEC TS 62443-1-1:2009, 3.2.70]

3.1.268**managed energy efficiency**

improvement of energy efficiency by systematic automated production management

[SOURCE: IEC TR 62837:2013, 3.3.7, modified – "energy management" replaced by "automated production management"]

3.1.269**manufacturing**

all life-cycle activities and procedures involved in the design, production, and support of manufacturing systems and of manufactured products

3.1.270**manufacturing application**

set of manufacturing processes, related resources and information exchange involved in the manufacture of a product or the provision of a service

[SOURCE: ISO 18435-1:2009, 3.14]

3.1.271**manufacturing facility**

site, or area within a site, that includes the resources within the site or area and includes the activities associated with the use of the resources

[SOURCE: IEC 62264-1:2013, 3.1.20]

3.1.272**manufacturing operations management****MOM**

activities within Level 3 of a manufacturing facility that coordinate the personnel, equipment and material in manufacturing

[SOURCE: IEC 62264-1:2013, 3.1.22]

3.1.273**manufacturing performance**

ability of a manufacturing system to achieve the intended results

3.1.274

manufacturing process

set of processes involving a flow and/or transformation of material, information, energy, control, or any other element in a manufacturing area

[SOURCE: ISO 18435-1:2009, 3.16, modified – "in manufacturing" deleted]

3.1.275

manufacturing support system

system which is used for providing the necessary other resource to a manufacturing system

[SOURCE: IEC TR 62837:2013, 3.7.4]

3.1.276

mapping

set of values having defined correspondence with the quantities or values of another set

[SOURCE: IEC 61804-2:2018, 3.1.53]

3.1.277

master data

data held by an organization that describes the entities that are both independent and fundamental for that organization and that it needs to reference in order to perform its transactions

3.1.278

master recipe

type of recipe that accounts for equipment capabilities and may include process cell-specific information.

[SOURCE: IEC 61512-1:1997, 3.29]

3.1.279

material

matter used in manufacturing the product

EXAMPLE: Raw materials, consumables, catalysts.

[SOURCE: ISO 15745-1:2003, 3.22]

3.1.280

material definition

definition of the properties for a substance

Note 1 to entry: This includes material that can be identified as raw, intermediate, final material, or consumable.

[SOURCE: IEC 62264-2:2013, 3.1.6]

3.1.281

material subplot

uniquely identifiable subset of a material lot

Note 1 to entry: This can be a single item.

[SOURCE: IEC 62264-2:2013, 3.1.7]

3.1.282**maximum value**

max

upper bound of a range of values in which the said value is meaningful

[SOURCE: IEC 61360-1:2017, 3.1.19, modified – Example and note deleted]

3.1.283**measurand**

particular quantity subject to measurement

[SOURCE: IEC 62714-2:2015, 3.1.3]

3.1.284**medium code**

abbreviation and identifier for the fluid running through a process

[SOURCE: IEC 62424:2016, 3.21, modified – "pipe" deleted]

3.1.285**manufacturing execution system****MES**

production control system with real-time processing

3.1.286**message**

structured information unit conveyed in a one-way transfer of data between one sending application to one or more receiving applications

[SOURCE: IEC 62264-5:2016, 3.1.3]

3.1.287**method**

implementation of an operation, which specifies the algorithm or procedure associated with an operation

[SOURCE: IEC TR 62390:2005, 3.1.17]

3.1.288**migration**

partial replacement of a component within an existing system configuration or extension of such configuration to modify functionality or technology

3.1.289**minimum value**

min

lower bound of a range of values in which the said value is meaningful

[SOURCE: IEC 61360-1:2017, 3.1.18, modified – Example and Note 1 to entry deleted]

3.1.290**mode**

the manner in which the transition of sequential functions are carried out within a procedural element or the accessibility for manipulating the states of equipment entities manually or by other types of control.

[SOURCE: IEC 61512-1:1997, 3.30]

3.1.291

model

representation of a real world process, device, or concept

[SOURCE: IEC 61804-2:2018, 3.1.54]

3.1.292

name

term which, in a given naming context, refers to an entity

[SOURCE: ISO 15745-1:2003, 3.25]

3.1.293

neutral database

vendor independent data storage system

[SOURCE: IEC 62424:2016, 3.23]

3.1.294

nominal value

nom

value of a quantity used to designate and identify a component, device, equipment, or system

3.1.295

non-quantitative property

property that identifies or describes an object by means of codes, abbreviations, names, references or descriptions

EXAMPLE Typical information content of non-quantitative properties is items such as codes, abbreviations, names, references, or descriptions.

[SOURCE: IEC 61360-1:2017, 3.1.21]

3.1.296

nonrepudiation

security service that provides protection against false denial of involvement in a communication

[SOURCE: IEC TS 62443-1-1:2009, 3.2.72]

3.1.297

obsolete product

not available product from the original producer to the original specification

[SOURCE: IEC 62890:2020, 3.1.29]

3.1.298

ontology

explicit and consensual specification of concepts of an application domain independent of any use of these concepts

[SOURCE: ISO 18435-3:2015, 3.1]

3.1.299**operations segment**

identification of personnel, equipment, physical assets, and material resources required to complete an operational step for a specific operations definition

[SOURCE: IEC 62264-1:2013, 3.1.25]

3.1.300**optimal control**

type of control for which the performance index reaches a largest or smallest value under specified conditions

3.1.301**optimize**

design a process or act upon a process such that the performance criterion used for evaluating the process states for a given task assumes a value either as large as possible or as small as possible within given limitations

[SOURCE: IEC 60050-351:2013, 351-43-14, modified – Note 1 to entry deleted]

3.1.302**orchestration of services**

flexible connection of individual services for a defined purpose

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

3.1.303**output**

product, material or energy flow that leaves a unit process

[SOURCE: IEC TR 62837:2013, 3.7.5]

3.1.304**output data**

data originating in a device, resource or functional element and transferred from them to external systems

[SOURCE: IEC TR 62390:2005, 3.1.21]

3.1.305**output variable**

variable whose value is established by one or more operations of a FB, and is supplied to a data output

Note 1 to entry: An output parameter of a FB, as defined in IEC 61131-3, is an output variable.

[SOURCE: IEC 61804-2:2018, 3.1.56]

3.1.306**outsider**

person or group not trusted with inside access, who may or may not be known to the targeted organization

Note 1 to entry: Outsiders may or may not have been insiders at one time.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.74]

3.1.307

parameter

property that describes the setting state of a system

Note 1 to entry: Parameters are properties carrying property magnitudes that are typically only changeable by an external setting. They are not changeable by internal system dynamics.

[SOURCE: DIN SPEC 92000:2020, 3.1.17]

3.1.308

peak shaving

process in an electrical system intended not to exceed a maximum overall energy demand

Note 1 to entry: Peak shaving can be obtained by planning of energy needs within the manufacturing system or load shedding or autonomous energy production.

[SOURCE: IEC TR 62837:2013, 3.3.8]

3.1.309

penetration

successful unauthorized access to a protected system resource

[SOURCE: IEC TS 62443-1-1:2009, 3.2.75]

3.1.310

personnel and environmental protection

the control activity that

- prevents events from occurring that would cause the process to react in a manner that would jeopardize personnel safety and/or harm the environment; and/or
- takes additional measures, such as starting standby equipment, to prevent an abnormal condition from proceeding to a more undesirable state that would jeopardize personnel safety and/or harm the environment.

[SOURCE: IEC 61512-1:1997, 3.33]

3.1.311

phase

lowest level of procedural element in the procedural control model

[SOURCE: IEC 61512-1:1997, 3.34]

3.1.312

phishing

type of security attack that lures victims to reveal information, by presenting a forged message to lure the recipient to a web site that looks like it is associated with a legitimate source

[SOURCE: IEC TS 62443-1-1:2009, 3.2.76, modified – "email" changed to "message"]

3.1.313

physical world

all actually existing objects and people

Note 1 to entry: The real world is the same as the physical world.

Note 2 to entry: Loaded or stored software is part of the physical world.

Note 3 to entry: The framework for considering each entirety needs to be defined.

[SOURCE: IEC PAS 63088:2017, 3.10]

3.1.314**plain text**

unencoded data that is input to, and transformed by an encryption process, or that is output by a decryption process

[SOURCE: IEC TS 62443-1-1:2009, 3.2.77]

3.1.315**planned time**

planned duration of a specific time period

EXAMPLE The intended duration of an operation or a resource state according to the planning.

[SOURCE: ISO 22400-2:2014, 2.2]

3.1.316**plant topology**

hierarchical structure of a plant, visualizable as object tree

[SOURCE: IEC 62714-1:2018, 3.1.20]

3.1.317**product life cycle management****PLM**

management and use of all the information generated throughout the life cycle of a product

3.1.318**plug & work**

setting up, modification or termination of interoperation between two or more involved parties with minimal effort

Note 1 to entry: The interoperability of those involved is assumed.

Note 2 to entry: The minimum effort can vary depending on the state of the art.

Note 3 to entry: Plug & play and plug & produce are synonyms or similar terms.

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

3.1.319**polymorphism**

pattern that allows substitution of a single concept in the same context by a different more specific (specialized) concept

Note 1 to entry: A specialised polymorphic block can replace a more generic one in the same context.

Note 2 to entry: A polymorphic operator (control property) can act in selecting between various specialisations.

[SOURCE: IEC 61360-1:2017, 3.1.22]

3.1.320**preventive maintenance**

maintenance carried out to mitigate degradation and reduce the probability of failure

Note 1 to entry: See also condition-based maintenance (192-06-07), and scheduled maintenance (192-06-12).

[SOURCE: IEC 60050-192:2015, 192-06-05]

3.1.321

primary energy

energy that has not been subjected to any conversion process

Note 1 to entry: Primary energy includes non-renewable energy and renewable energy. The sum of primary energy from all energy sources may be called total primary energy.

[SOURCE: IEC TR 62837:2013, 3.1.5]

3.1.322

privilege

authorization or set of authorizations to perform specific functions, especially in the context of a computer operating system

EXAMPLE Functions that are controlled through the use of privilege include acknowledging alarms, changing setpoints, modifying control algorithms.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.78]

3.1.323

procedural control

control that directs equipment-oriented actions to take place in an ordered sequence in order to carry out some process-oriented task

[SOURCE: IEC 61512-1:1997, 3.35]

3.1.324

procedural element

building block for procedural control that is defined by the procedural control model

[SOURCE: IEC 61512-1:1997, 3.36]

3.1.325

procedure

strategy for carrying out a process

Note 1 to entry: In general, this refers to the strategy for making a batch within a process cell. It may also refer to a process that does not result in the production of a product, such as a clean-in-place procedure.

[SOURCE: IEC 61512-1:1997, 3.37]

3.1.326

procedure function chart

graphical representation of a recipe procedure that specifies the processing order for recipe procedural elements

[SOURCE: IEC 61512-2:2001, 3.6]

3.1.327

process

set of activities performed with a set of resources to realize an objective within a specified timeline

[SOURCE: ISO 22400-1:2014, 2.1.8]

3.1.328**process action**

minor processing activities that are combined to make up a process operation

Note 1 to entry: Process actions are the lowest level of processing activity within the process model.

[SOURCE: IEC 61512-1:1997, 3.39]

3.1.329**process cell**

logical grouping of equipment that includes the equipment required for production of one or more batches. It defines the span of logical control of one set of process equipment within an area

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

[SOURCE: IEC 61512-1:1997, 3.40]

3.1.330**process control**

control activity that includes the functions needed to provide sequential, regulatory and discrete control, and to gather and display data

[SOURCE: IEC 61512-1:1997, 3.41, modified – "control" deleted]

3.1.331**process control function**

function to work on process variables quantities, which is composed of basic functions of process control, specific to units of the plant

Note 1 to entry: In addition to process control functions associated with specific control levels, there can also be process control functions that link input and output variables across several control levels. For instance, a process control function in the feedback path with the controlled variable as input variable and the manipulated variable as output variable, describes the action path from the sensor via the controller to the final controlling element. Another process control function connects the operator with the indicators for the process variables. In view of the diversity of definitions of process control functions, standardization is not appropriate at this time.

[SOURCE: IEC 60050-351:2013, 351-55-16]

3.1.332**process input**

identification and quantity of a raw material or other resource required to make a product

[SOURCE: IEC 61512-1:1997, 3.42]

3.1.333**process management**

control activity that includes the control functions needed to manage batch production within a process cell

[SOURCE: IEC 61512-1:1997, 3.43]

3.1.334**process operation**

major processing activity that usually results in a chemical or physical change in the material being processed and that is defined without consideration of the actual target equipment configuration

[SOURCE: IEC 61512-1:1997, 3.44]

3.1.335

process output

identification and quantity of material or energy expected to result from one execution of a control recipe

[SOURCE: IEC 61512-1:1997, 3.45]

3.1.336

process parameter

information that is needed to manufacture a material but does not fall into the classification of process input or process output

Note 1 to entry: Examples of process parameter information are temperature, pressure and time.

[SOURCE: IEC 61512-1:1997, 3.46]

3.1.337

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]

3.1.338

process stage

part of a process that operates independently and that results in a planned sequence of chemical or physical changes in the material being processed

[SOURCE: IEC 61512-1:1997, 3.47, modified – "usually" and "from other process stages" removed]

3.1.339

processing function

function in a process

Note 1 to entry: A processing function serves a control module according to IEC 61512-1:1997, 3.10 and 5.2.2.4.

[SOURCE: IEC 62424:2016, 3.34]

3.1.340

producer

company which develops a product type, maintains it during the life cycle and manufactures instances of this type

[SOURCE: IEC 62890:2020, 3.1.30]

3.1.341

product

result of labour or of a natural or industrial process

[SOURCE: IEC 61360-1:2017, 3.1.23]

3.1.342**product abandonment**

end of all deliveries and service for a product

3.1.343**product definition**

identification of personnel, equipment, physical assets, and material resources, production rules and scheduling required to create a product which includes a reference to a bill of materials, a product production rule, and a bill of resources

[SOURCE: IEC 62264-1:2013, 3.1.28]

3.1.344**product segment**

identification of personnel, equipment, physical asset, and material resources required of a process segment to complete a production step for a specific product

[SOURCE: IEC 62264-1:2013, 3.1.29]

3.1.345**production capability**

capability of resources to perform production and the capacity of those resources

EXAMPLE 1 Includes the collection of personnel, equipment, material, and process segment capabilities.

EXAMPLE 2 Includes the sum total of the current committed, available, and unattainable capacity of the production facility.

EXAMPLE 3 Includes the highest sustainable output rate that could be achieved for a given product mix, raw materials, worker effort, plant, and equipment.

[SOURCE: IEC 62264-1:2013, 3.1.30]

3.1.346**production control**

collection of functions that manage all production within a site or area

[SOURCE: IEC 62264-1:2013, 3.1.31]

3.1.347**production line**

collection of equipment dedicated to the manufacture of a specific number of products or product families

Note 1 to entry: A production line is a type of work center.

[SOURCE: IEC 62264-1:2013, 3.1.32]

3.1.348**production rules**

information used to instruct a manufacturing operation how to produce a product

[SOURCE: IEC 62264-1:2013, 3.1.34]

3.1.349

production segment

sequence of process segments and product segments

Note 1 to entry: See IEC 62264-2.

[SOURCE: ISO 18435-1:2009, 3.20]

3.1.350

production system

system intended for production of goods

Note 1 to entry: The concept of production system includes spare parts.

Note 2 to entry: The concept of production system does not encompass the whole manufacturing facility. It excludes in particular the supporting infrastructure (such as building, power distribution, lighting, ventilation). It also excludes financial assets, human resources, raw process materials, energy, work pieces in process, end products.

Note 3 to entry: Production systems can support different types of production processes (continuous, batch, or discrete).

[SOURCE: IEC 62832-1:2020, 3.1.24]

3.1.351

production unit

collection of equipment that converts, separates, or reacts one or more feedstocks to produce intermediate or final products

Note 1 to entry: A production unit is a type of work center.

[SOURCE: IEC 62264-1:2013, 3.1.35]

3.1.352

profile

<automation> set of one or more base specifications and/or sub-profiles, and, where applicable, the identification of chosen classes, conforming subsets, options and parameters of those base specifications, or sub-profiles necessary to accomplish a particular function, activity, or relationship

[SOURCE: ISO 15745-1:2003, 3.28]

3.1.353

property

data element type

defined parameter suitable for the description and differentiation of objects

Note 1 to entry: A property describes one characteristic of a given object.

Note 2 to entry: A property can have attributes such as code, version, and revision.

Note 3 to entry: The specification of a property can include predefined choices of values.

[SOURCE: IEC 61360-1:2017, 3.1.24]

3.1.354

proprietary database

vendor specific data storage system, with syntax and/or semantic not complying to any standard

[SOURCE: IEC 62424:2016, 3.35]

3.1.355**protocol**

set of formal rules describing how to exchange data between entities

3.1.356**public key certificate**

set of data that uniquely identifies an entity, contains the entity's public key, and is digitally signed by a trusted party, thereby binding the public key to the entity

3.1.357**quantitative property**

property with a numerical value representing a physical quantity, a quantity of information or a count of objects

[SOURCE: IEC 61360-1:2017, 3.1.25]

3.1.358**quantity**

property of a phenomenon, body, or substance, where the property has a magnitude that can be expressed by means of a number and a reference

Note 1 to entry: The generic concept "quantity" can be divided into several levels of specific concepts.

[SOURCE: IEC 61360-1:2017, 3.1.26, modified – amended the Note to entry]

3.1.359**reasonably foreseeable misuse**

use of a product or system in a way not intended by the supplier, but which can result from readily predictable human behaviour

Note 1 to entry: Readily predictable human behaviour includes the behaviour of all types of users, e.g. the elderly, children and persons with disabilities. For more information, see ISO 10377.

Note 2 to entry: In the context of consumer safety, the term "reasonably foreseeable use" is increasingly used as a synonym for both "intended use" and "reasonably foreseeable misuse".

[SOURCE: ISO/IEC GUIDE 51:2014, 3.7]

3.1.360**recipe**

necessary set of information that uniquely defines the production requirements for a specific product.

Note 1 to entry: There are four types of recipes defined in this document: general, site, master and control.

[SOURCE: IEC 61512-1:1997, 3.48]

3.1.361**recipe element**

structural entity that is used to represent recipe entities and symbols, except transitions and directed links, that are used in procedure function charts

[SOURCE: IEC 61512-2:2001, 3.7]

3.1.362

recipe entity

combination of a procedural element with an associated recipe information (for example, header, formula, equipment requirements, other information)

Note 1 to entry: General, site, master and control recipes are also recipe entities.

[SOURCE: IEC 61512-2:2001, 3.8, modified – Second sentence changed to a Note to entry]

3.1.363

recipe management

control activity that includes the control functions needed to create, store and maintain general, site and master recipes

[SOURCE: IEC 61512-1:1997, 3.49]

3.1.364

re-design

life-cycle management strategy in which a new version of a product type is developed which typically fulfills or exceeds the specification, and therefore the compatibility profile, of a previous type

[SOURCE: IEC 62890:2020, 3.1.35]

3.1.365

reference architecture

architecture description that provides a proven template solution when developing or validating an architecture for a particular solution

[SOURCE: IEC 60050-741:2020, 741-01-27]

3.1.366

reference designation

identifier of a specific object formed with respect to the system of which the object is a constituent, based on one or more aspects of that system

Note 1 to entry: Terms "object", "aspect" and "system" are also defined in IEC 81346-1:2009, respectively at 3.1, 3.3 and 3.2.

[SOURCE: IEC 62424:2016, 3.37]

3.1.367

reference model

model that is generally used and recognized as being suitable (has recommendation character) for deriving specific models

[SOURCE: IEC PAS 63088:2017, 3.12]

3.1.368

reference time

base timeline used for time constrained models, corresponding to the planned maximum time interval available for production and maintenance tasks

EXAMPLE: A calendar day with 24 hours; a week.

[SOURCE: ISO 22400-2:2014, 2.1, modified – "constrained" added]

3.1.369
relation

aspect or quality that connects two or more things or parts as being or belonging together

[SOURCE: IEC 61360-1:2017, 3.1.27]

3.1.370
releases

emissions to air and discharges to water and soil

[SOURCE: IEC TR 62837:2013, 3.7.8]

3.1.371
reliability

ability of a system to perform a required function under stated conditions for a specified period of time

[SOURCE: IEC TS 62443-1-1:2009, 3.2.82]

3.1.372
remote access

use of systems that are inside the perimeter of the security zone being addressed from a different geographical location with the same rights as when physically present at the location

Note 1 to entry: The exact definition of "remote" can vary according to the situation. For example, access may come from a location that is remote to the specific zone, but still within the boundaries of a company or organization. This might represent a lower risk than access that originates from a location that is remote and outside of a company's boundaries.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.83]

3.1.373
remote client

asset outside the control network that is temporarily or permanently connected to a host inside the control network via a communication link in order to directly or indirectly access parts of the control equipment on the control network

[SOURCE: IEC TS 62443-1-1:2009, 3.2.84]

3.1.374
repudiation

denial by one of the entities involved in a communication of having participated in all or part of the communication

[SOURCE: IEC TS 62443-1-1:2009, 3.2.85]

3.1.375
requirement

provision that conveys criteria to be fulfilled

[SOURCE: ISO/IEC Guide 2:2004, 7.5]

3.1.376
residual risk

remaining risk after the safety/security controls or countermeasures have been applied

[SOURCE: IEC TS 62443-1-1:2009, 3.2.86, modified – Added "safety"]

3.1.377

resilience

ability of an IACS organization, process entity or system, to resist being affected by disruptions

3.1.378

resource

asset that is utilized or consumed during the execution of a process

Note 1 to entry: Resources may include diverse entities such as personnel, facilities, capital equipment, tools, and utilities such as power, water, fuel and communication infrastructures.

Note 2 to entry: Resources may be reusable, renewable or consumable.

3.1.379

resource management application

application whose primary function is the management of a single resource

[SOURCE: IEC 61804-2:2018, 3.1.62]

3.1.380

resource relationship network

one or more expressions of a relationship between two or more resources

[SOURCE: IEC 62264-4:2015, 3.1.6]

3.1.381

revision

defined status of a software or hardware, including all of its integrated components, which is explicitly identified

Note 1 to entry: The explicit identifier is typically a revision number.

Note 2 to entry: All revisions should be unique.

[SOURCE: IEC 62890:2020, 3.1.37, modified – "by a revision number" deleted and Notes to entry added]

3.1.382

risk

combination of the probability of occurrence of harm and the severity of that harm

3.1.383

risk analysis

systematic use of available information to identify hazards and to estimate the risk

[SOURCE: ISO/IEC GUIDE 51:2014, 3.10]

3.1.384

risk assessment

process that systematically identifies potential vulnerabilities to valuable system resources and threats to those resources, quantifies loss exposures and consequences based on probability of occurrence, and (optionally) recommends how to allocate resources to countermeasures to minimize total exposure

Note 1 to entry: Types of resources include physical, logical and human.

Note 2 to entry: Risk assessments are often combined with vulnerability assessments to identify vulnerabilities and quantify the associated risk. They are carried out initially and periodically to reflect changes in the organization's risk tolerance, vulnerabilities, procedures, personnel and technological changes.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.88]

3.1.385**risk evaluation**

procedure based on the risk analysis to determine whether tolerable risk has been exceeded

[SOURCE: ISO/IEC GUIDE 51:2014, 3.12]

3.1.386**risk management**

process of identifying and applying countermeasures commensurate with the value of the assets protected, based on a risk assessment

[SOURCE: IEC TS 62443-1-1:2009, 3.2.89]

3.1.387**risk mitigation controls**

combination of countermeasures and business continuity plans to manage risk

[SOURCE: IEC TS 62443-1-1:2009, 3.2.90, modified – "to manage risk" added]

3.1.388**risk reduction measure****protective measure**

action or means to eliminate hazards or reduce risks

EXAMPLE Inherently safe design; protective devices; personal protective equipment; information for use and installation; organization of work; training; application of equipment; supervision.

[SOURCE: ISO/IEC GUIDE 51:2014, 3.13]

3.1.389**risk tolerance level**

level of residual risk that is acceptable to an organization

[SOURCE: IEC TS 62443-1-1:2009, 3.2.91]

3.1.390**robot****industrial robot**

automatically controlled, reprogrammable, multipurpose manipulator, programmable in three or more axes, which can be either fixed in place or mobile for use in industrial automation applications

[SOURCE: IEC 62714-2:2015, 3.1.1]

3.1.391**robustness**

capability of a system to continue to fulfill its function under changing conditions

[SOURCE: IEC 62890:2020, 3.1.38]

3.1.392**role**

set of characteristics that distinguish a resource's ability to exhibit a set of required behaviours

[SOURCE: ISO 18435-1:2009, 3.22]

3.1.393

router

network component that establishes a path through one or more computer networks and forwards packets

Note 1 to entry: In OSI conforming computer networks, a router operates at the network layer.

[SOURCE: IEC 60050-732: 2010, 732-01-18, modified – "functional unit" replaced by "network component"]

3.1.394

safety

freedom from risk which is not tolerable

3.1.395

safety integrity level

discrete level (one out of four levels) for specifying the safety integrity requirements of the safety-instrumented functions to be allocated to the safety-instrumented systems

Note 1 to entry: Safety integrity level 4 has the highest level of safety integrity; safety integrity level 1 has the lowest.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.96]

3.1.396

safety network

network that connects safety-instrumented systems for the communication of safety-related information

[SOURCE: IEC TS 62443-1-1:2009, 3.2.97]

3.1.397

safety-instrumented system

system used to implement one or more safety-instrumented functions

Note 1 to entry: A safety-instrumented system is composed of any combination of sensor(s), logic solver(s), and actuator(s).

[SOURCE: IEC TS 62443-1-1:2009, 3.2.95]

3.1.398

secret

condition of information being protected from being known by any system entities except those intended to know it

[SOURCE: IEC TS 62443-1-1:2009, 3.2.98]

3.1.399

security

- a) measures taken to protect a system
- b) condition of a system that results from the establishment and maintenance of measures to protect the system
- c) condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss
- d) capability of a computer-based system to provide adequate confidence that unauthorized persons and systems can neither modify the software and its data nor gain access to the system functions, and yet to ensure that this is not denied to authorized persons and systems

- e) prevention of illegal or unwanted penetration of, or interference with the proper and intended operation of an industrial automation and control system

Note 1 to entry: Measures can be controls related to physical security (controlling physical access to computing assets) or logical security (capability to login to a given system and application).

[SOURCE: IEC TS 62443-1-1:2009, 3.2.99]

3.1.400

security architecture

plan and set of principles describing the security services that a system is required to provide to meet the needs of its users, the system elements required to implement the services, and the performance levels required in the elements to deal with the threat environment

Note 1 to entry: In this context, security architecture would be an architecture to protect the control network from intentional or unintentional security events.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.100]

3.1.401

security audit

independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures

[SOURCE: IEC TS 62443-1-1:2009, 3.2.101]

3.1.402

security control

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 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, 3.2.103, modified – Different Note]

3.1.403

security components

assets such as firewalls, authentication modules, or encryption software used to improve the security performance of an industrial automation and control system

[SOURCE: IEC TS 62443-1-1:2009, 3.2.102]

3.1.404

security event

occurrence in a system that is relevant to the security of the system

[SOURCE: IEC TS 62443-1-1:2009, 3.2.104]

3.1.405

security function

function of a zone or conduit to prevent unauthorized electronic intervention that can impact or influence the normal functioning of devices and systems within the zone or conduit

[SOURCE: IEC TS 62443-1-1:2009, 3.2.105]

3.1.406

security intrusion

security event or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system (or system resource) without having authorization to do so

[SOURCE: IEC TS 62443-1-1:2009, 3.2.107]

3.1.407

security level

level corresponding to the required effectiveness of countermeasures and inherent security properties of devices and systems for a zone or conduit based on assessment of risk for the zone or conduit

Note 1 to entry: There are four levels with 1 being lowest and 4 highest.

SL 1 – Prevent the unauthorized disclosure of information via eavesdropping or casual exposure.

SL 2 – Prevent the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, generic skills and low motivation.

SL 3 – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, IACS specific skills and moderate motivation.

SL 4 – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extended resources, IACS specific skills and high motivation.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.108, modified – Note to entry added]

3.1.408

security objective

aspect of security whose purpose is to use certain mitigation measures, such as confidentiality, integrity, availability, user authenticity, access authorization, accountability, etc.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.109]

3.1.409

security performance

program's compliance, completeness of measures to provide specific threat protection, post-compromise analysis, review of changing business requirements, new threat and vulnerability information, and periodic audit of control systems to ensure security measures remain effective and appropriate

Note 1 to entry: Tests, audits, tools, measures, or other methods are required to evaluate security practice performance.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.111]

3.1.410

security perimeter

boundary (logical or physical) of the domain in which a security policy or security architecture applies, i.e., the boundary of the space in which security services protect system resources

[SOURCE: IEC TS 62443-1-1:2009, 3.2.110]

3.1.411

security policy

set of rules that specify or regulate how a system or organization provides security services to protect its assets

[SOURCE: IEC TS 62443-1-1:2009, 3.2.112]

3.1.412**security procedures**

definitions stating exactly how practices are implemented and executed

Note 1 to entry: Security procedures are implemented through personnel training and actions using currently available and installed technology.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.113]

3.1.413**security program**

combination of all aspects of managing security, ranging from the definition and communication of policies through implementation of best industry practices, ongoing operation and auditing

[SOURCE: IEC TS 62443-1-1:2009, 3.2.114]

3.1.414**security services**

mechanisms used to provide confidentiality, data integrity, authentication, or no repudiation of information

[SOURCE: IEC TS 62443-1-1:2009, 3.2.115]

3.1.415**security violation**

act or event that disobeys or otherwise breaches security policy through an intrusion or the actions of a well-meaning insider

[SOURCE: IEC TS 62443-1-1:2009, 3.2.116]

3.1.416**security zone**

grouping of logical or physical assets that share common security requirements

Note 1 to entry: All unqualified uses of the term "zone" in this document should be assumed to refer to a security zone.

Note 2 to entry: A zone has a clear border with other zones. The security policy of a zone is typically enforced by a combination of mechanisms both at the zone edge and within the zone. Zones can be hierarchical in the sense that they can be comprised of a collection of sub-zones.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.117]

3.1.417**self-checking**

built-in facility for detecting errors in its own function

[SOURCE: IEC 60050-192:2015, 192-10-10]

3.1.418**self-recoverability**

ability to recover from a failure, without external action

[SOURCE: IEC 60050-192:2015, 192-01-26, modified – Note 1 to entry deleted]

3.1.419

self-testing

built-in test facility for assessing internal system status

[SOURCE: IEC 60050-192:2015, 192-10-11, modified – Note 1 to entry deleted]

3.1.420

sensing element

functional unit that senses the effect of a measured variable at its input and places a corresponding measurement signal at its output

Note 1 to entry: The corresponding physical unit is named sensor or detecting device.

Note 2 to entry: Examples of sensors are

- a) thermocouple
- b) foil strain gauge
- c) pH electrode.

[SOURCE: IEC 60050-351:2013, 351-56-26, modified – New Note 1 to entry, Examples restructured into Note 2 to entry]

3.1.421

sensor

unit that detects objects or obstacles in its monitoring range or that is affected by a measurand and which provides an electrical signal or data representing the detection or the measurement

EXAMPLE Limit switch, proximity sensor, pressure transmitter, vibration transducer, strain gauge, photo detector.

[SOURCE: IEC 62714-2:2015, 3.1.2]

3.1.422

server

device or application that provides information or services to client applications and devices

[SOURCE: IEC TS 62443-1-1:2009, 3.2.119]

3.1.423

service

distinct part of the functionality that is provided by an entity through interfaces

[SOURCE: IEC 60050-741:2020, 741-01-28]

3.1.424

service provider

organization or part of an organization that manages and delivers a service or services to the customer

Note 1 to entry: In the definition "organization" means "person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives"

3.1.425

service orientation

paradigm which enables the straightforward exchange, addition or removal of loosely coupled services

3.1.426

shared-use resource

common resource that can be used by more than one user at a time

[SOURCE: IEC 61512-1:1997, 3.54]

3.1.427**signal compatibility**

level of compatibility from the function view of the compatibility profile related to signal acquisition and processing

[SOURCE: IEC 62890:2020, 3.1.42]

3.1.428**site**

identified physical, geographical, and/or logical component grouping of a manufacturing enterprise

[SOURCE: IEC 62264-1:2013, 3.1.39]

3.1.429**site recipe**

type of recipe that is site-specific

[SOURCE: IEC 61512-1:1997, 3.56, modified – Note deleted]

3.1.430**situation**

large number of dynamic objects that change state in time and space and engage each other into complex spatio-temporal relationships.

3.1.431**situation management**

synergistic goal-directed process of:

- (a) sensing and information collection,
- (b) perceiving and recognizing situations,
- (c) analyzing past situations and predicting future situations, and
- (d) reasoning, planning and implementing actions so that desired goal situation is reached within some pre-defined constraints

3.1.432**smart**

capable of some independent action

3.1.433**smart factory**

factory whose degree of integration has reached a level which makes self-organizing functions possible in production and in associated business processes relating to production

Note 1 to entry: The virtual representation of the factory makes intelligent decisions possible. The aim is to increase efficiency, effectiveness, flexibility and/or adaptability.

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

3.1.434**smart manufacturing**

manufacturing that improves its performance aspects with integrated and intelligent use of processes and resources in cyber, physical and human spheres to create and deliver products and services, which also collaborates with other domains within enterprises' value chains

Note 1 to entry: Performance aspects include agility, efficiency, safety, security, sustainability or any other performance indicators identified by the enterprise.

Note 2 to entry: In addition to manufacturing, other enterprise domains can include engineering, logistics, marketing, procurement, sales or any other domains identified by the enterprise.

3.1.435

smart product

produced or manufactured (intermediate) product which in a smart factory delivers the (outward) communication capability to network and to interact intelligently with other production participants

Note 1 to entry: The product is a produced or manufactured article or semi-finished product.

Note 2 to entry: A digital image is part of the product intelligence and can be localized on the product itself but also spatially separate from it.

Note 3 to entry: Unique identification and product-related information makes it possible for the product to be linked to the smart factory.

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

3.1.436

smart production

dramatic increases in production from how an entity engages with supply chains, applies collaborative leadership methods, works across disciplines and systems, and how production uses data and integrated technologies for accelerated improvements.

Note 1 to entry: Adaption of the ISO TMB SAG working definition of what a Smart City should be: "Productivity": the ratio of work product to work effort. ISO/IEC 20926:2009.

3.1.437

software

intellectual creation comprising the programs, procedures, rules and any associated documentation pertaining to the operation of a system

[SOURCE: IEC 61804-2:2018, 3.1.64]

3.1.438

software compatibility

level of compatibility from the function view of the compatibility profile related to software

[SOURCE: IEC 62890:2020, 3.1.43]

3.1.439

source database

data storage system of the source tool

[SOURCE: IEC 62424:2016, 3.40]

3.1.440

specific energy consumption

energy consumption per physical unit of output

EXAMPLE Gigajoule (GJ) per ton of steel, Btu/ton of product, annual kWh per m².

[SOURCE: IEC TR 62837:2013, 3.3.10]

3.1.441

spoof

pretending to be an authorized user and performing an unauthorized action