



BSI Standards Publication

Industrial communication networks — Network and system security

Part 1-1: Terminology, concepts and models

National foreword

This Published Document is the UK implementation of IEC/TS 62443-1-1:2009.

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

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

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2023
Published by BSI Standards Limited 2023

ISBN 978 0 539 27005 1

ICS 25.040.40; 33.040.40; 35.040.01

Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 May 2023.

Amendments/corrigenda issued since publication

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



IEC/TS 62443-1-1

Edition 1.0 2009-07

TECHNICAL SPECIFICATION



**Industrial communication networks – Network and system security –
Part 1-1: Terminology, concepts and models**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE **XC**

ICS 25.040.40; 33.040.040; 35.040

ISBN 978-2-88910-710-0

CONTENTS

FOREWORD.....	5
INTRODUCTION.....	7
1 Scope.....	8
1.1 General.....	8
1.2 Included functionality.....	8
1.3 Systems and interfaces.....	8
1.4 Activity-based criteria.....	9
1.5 Asset-based criteria.....	9
2 Normative references.....	10
3 Terms, definitions and abbreviations.....	10
3.1 General.....	10
3.2 Terms and definitions.....	10
3.3 Abbreviations.....	26
4 The situation.....	27
4.1 General.....	27
4.2 Current systems.....	27
4.3 Current trends.....	28
4.4 Potential impact.....	28
5 Concepts.....	29
5.1 General.....	29
5.2 Security objectives.....	29
5.3 Foundational requirements.....	30
5.4 Defence in depth.....	30
5.5 Security context.....	30
5.6 Threat-risk assessment.....	32
5.6.1 General.....	32
5.6.2 Assets.....	32
5.6.3 Vulnerabilities.....	34
5.6.4 Risk.....	34
5.6.5 Threats.....	36
5.6.6 Countermeasures.....	38
5.7 Security program maturity.....	39
5.7.1 Overview.....	39
5.7.2 Maturity phases.....	42
5.8 Policies.....	45
5.8.1 Overview.....	45
5.8.2 Enterprise level policy.....	46
5.8.3 Operational policies and procedures.....	47
5.8.4 Topics covered by policies and procedures.....	47
5.9 Security zones.....	50
5.9.1 General.....	50
5.9.2 Determining requirements.....	50
5.10 Conduits.....	51
5.10.1 General.....	51
5.10.2 Channels.....	52
5.11 Security levels.....	53

5.11.1	General	53
5.11.2	Types of security levels.....	53
5.11.3	Factors influencing SL(achieved) of a zone or conduit	55
5.11.4	Impact of countermeasures and inherent security properties of devices and systems	57
5.12	Security level lifecycle.....	57
5.12.1	General	57
5.12.2	Assess phase	58
5.12.3	Develop and implement phase	59
5.12.4	Maintain phase	60
6	Models	61
6.1	General	61
6.2	Reference models	62
6.2.1	Overview	62
6.2.2	Reference model levels.....	63
6.3	Asset models.....	65
6.3.1	Overview	65
6.3.2	Enterprise.....	68
6.3.3	Geographic sites.....	68
6.3.4	Area	68
6.3.5	Lines, units, cells, vehicles.....	68
6.3.6	Supervisory control equipment	68
6.3.7	Control equipment	68
6.3.8	Field I/O network	69
6.3.9	Sensors and actuators	69
6.3.10	Equipment under control	69
6.4	Reference architecture	69
6.5	Zone and conduit model.....	69
6.5.1	General	69
6.5.2	Defining security zones	70
6.5.3	Zone identification	70
6.5.4	Zone characteristics.....	74
6.5.5	Defining conduits	76
6.5.6	Conduit characteristics.....	77
6.6	Model relationships.....	79
	Bibliography	81
	Figure 1 – Comparison of objectives between IACS and general IT systems	29
	Figure 2 – Context element relationships	31
	Figure 3 – Context model	31
	Figure 4 – Integration of business and IACS cybersecurity.....	40
	Figure 5 – Cybersecurity level over time	40
	Figure 6 – Integration of resources to develop the CSMS.....	41
	Figure 7 – Conduit example.....	52
	Figure 8 – Security level lifecycle.....	58
	Figure 9 – Security level lifecycle – Assess phase	59
	Figure 10 – Security level lifecycle – Implement phase	60
	Figure 11 – Security level lifecycle – Maintain phase.....	61

Figure 12 – Reference model for IEC 62443 standards	62
Figure 13 – SCADA reference model	63
Figure 14 – Process manufacturing asset model example.....	66
Figure 15 – SCADA system asset model example.....	67
Figure 16 – Reference architecture example.....	69
Figure 17 – Multiplant zone example	71
Figure 18 – Separate zones example.....	72
Figure 19 – SCADA zone example.....	73
Figure 20 – SCADA separate zones example.....	74
Figure 21 – Enterprise conduit.....	77
Figure 22 – SCADA conduit example.....	78
Figure 23 – Model relationships.....	80
Table 1 – Types of loss by asset type	33
Table 2 – Security maturity phases	43
Table 3 – Concept phase	43
Table 4 – Functional analysis phase	43
Table 5 – Implementation phase.....	44
Table 6 – Operations phase	44
Table 7 – Recycle and disposal phase.....	45
Table 8 – Security levels	53

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**INDUSTRIAL COMMUNICATION NETWORKS –
NETWORK AND SYSTEM SECURITY –****Part 1-1: Terminology, concepts and models**

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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
- 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.

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a technical specification when

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
- the subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC 62443-1-1, which is a technical specification, has been prepared by IEC technical committee 65: Industrial-process measurement, control and automation.

This technical specification is derived from the corresponding US ANSI/S99.01.01 standard.

The text of this technical specification is based on the following documents:

Enquiry draft	Report on voting
65/423/DTS	65/432A/RVC

Full information on the voting for the approval of this technical specification can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts of the IEC 62433 series, published under the general title *Industrial communication networks – Network and system security*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

- transformed into an International standard,
- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

NOTE The revision of this technical specification will be synchronized with the other parts of the IEC 62443 series.

IMPORTANT – The “colour inside” logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this publication using a colour printer.

INTRODUCTION

The subject of this technical specification is security for industrial automation and control systems. In order to address a range of applications (i.e., industry types), each of the terms in this description have been interpreted very broadly.

The term “Industrial Automation and Control Systems” (IACS), includes control systems used in manufacturing and processing plants and facilities, building environmental control systems, geographically dispersed operations such as utilities (i.e., electricity, gas, and water), pipelines and petroleum production and distribution facilities, and other industries and applications such as transportation networks, that use automated or remotely controlled or monitored assets.

The term “security” is considered here to mean the prevention of illegal or unwanted penetration, intentional or unintentional interference with the proper and intended operation, or inappropriate access to confidential information in IACS. Cybersecurity which is the particular focus of this technical specification, includes computers, networks, operating systems, applications and other programmable configurable components of the system.

The audience for this technical specification includes all users of IACS (including facility operations, maintenance, engineering, and corporate components of user organizations), manufacturers, suppliers, government organizations involved with, or affected by, control system cybersecurity, control system practitioners, and security practitioners. Because mutual understanding and cooperation between information technology (IT) and operations, engineering, and manufacturing organizations is important for the overall success of any security initiative, this technical specification is also a reference for those responsible for the integration of IACS and enterprise networks.

Typical questions addressed by this technical specification include:

- a) What is the general scope of application for IACS security?
- b) How can the needs and requirements of a security system be defined using consistent terminology?
- c) What are the basic concepts that form the foundation for further analysis of the activities, system attributes, and actions that are important to provide electronically secure control systems?
- d) How can the components of an IACS be grouped or classified for the purpose of defining and managing security?
- e) What are the different cybersecurity objectives for control system applications?
- f) How can these objectives be established and codified?

Each of these questions is addressed in detail in subsequent clauses of this technical specification.

INDUSTRIAL COMMUNICATION NETWORKS – NETWORK AND SYSTEM SECURITY –

Part 1-1: Terminology, concepts and models

1 Scope

1.1 General

This part of the IEC 62443 series is a technical specification which defines the terminology, concepts and models for Industrial Automation and Control Systems (IACS) security. It establishes the basis for the remaining standards in the IEC 62443 series.

To fully articulate the systems and components the IEC 62443 series address, the range of coverage may be defined and understood from several perspectives, including the following:

- a) range of included functionality;
- b) specific systems and interfaces;
- c) criteria for selecting included activities;
- d) criteria for selecting included assets.

Each of these is described in the following subclauses:

1.2 Included functionality

The scope of this technical specification can be described in terms of the range of functionality within an organization's information and automation systems. This functionality is typically described in terms of one or more models.

This technical specification focuses primarily on industrial automation and control, as described in a reference model (see Clause 6). Business planning and logistics systems are not explicitly addressed within the scope of this technical specification, although the integrity of data exchanged between business and industrial systems is considered.

Industrial automation and control includes the supervisory control components typically found in process industries. It also includes SCADA (Supervisory Control and Data Acquisition) systems that are commonly used by organizations that operate in critical infrastructure industries. These include the following:

- a) electricity transmission and distribution;
- b) gas and water distribution networks;
- c) oil and gas production operations;
- d) gas and liquid transmission pipelines.

This is not an exclusive list. SCADA systems may also be found in other critical and non-critical infrastructure industries.

1.3 Systems and interfaces

In encompassing all IACS, this technical specification covers systems that can affect or influence the safe, secure, and reliable operation of industrial processes. They include, but are not limited to:

- a) Industrial control systems and their associated communications networks¹, including distributed control systems (DCSs), programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices, SCADA systems, networked electronic sensing and control, metering and custody transfer systems, and monitoring and diagnostic systems. (In this context, industrial control systems include basic process control system and Safety-Instrumented System (SIS) functions, whether they are physically separate or integrated.)
- b) Associated systems at level 3 or below of the reference model described in Clause 6. Examples include advanced or multivariable control, online optimizers, dedicated equipment monitors, graphical interfaces, process historians, manufacturing execution systems, pipeline leak detection systems, work management, outage management, and electricity energy management systems.
- c) Associated internal, human, network, software, machine or device interfaces used to provide control, safety, manufacturing, or remote operations functionality to continuous, batch, discrete, and other processes.

1.4 Activity-based criteria

IEC 62443-2-1² provides criteria for defining activities associated with manufacturing operations. A similar list has been developed for determining the scope of this technical specification. A system should be considered to be within the range of coverage of the IEC 62443 series if the activity it performs is necessary for any of the following:

- a) predictable operation of the process;
- b) process or personnel safety;
- c) process reliability or availability;
- d) process efficiency;
- e) process operability;
- f) product quality;
- g) environmental protection;
- h) regulatory compliance;
- i) product sales or custody transfer.

1.5 Asset-based criteria

The coverage of this technical specification includes those systems in assets that meet any of the following criteria, or whose security is essential to the protection of other assets that meet these criteria:

- a) The asset has economic value to a manufacturing or operating process.
- b) The asset performs a function necessary to operation of a manufacturing or operating process.
- c) The asset represents intellectual property of a manufacturing or operating process.
- d) The asset is necessary to operate and maintain security for a manufacturing or operating process.
- e) The asset is necessary to protect personnel, contractors, and visitors involved in a manufacturing or operating process.
- f) The asset is necessary to protect the environment.

¹ The term “communications networks” includes all types of communications media, including various types of wireless communications. A detailed description of the use of wireless communications in industrial automation systems is beyond the scope of this technical specification. Wireless communication techniques are specifically mentioned only in situations where their use or application may change the nature of the security applied or required.

² To be published.

- g) The asset is necessary to protect the public from events caused by a manufacturing or operating process.
- h) The asset is a legal requirement, especially for security purposes of a manufacturing or operating process.
- i) The asset is needed for disaster recovery.
- j) The asset is needed for logging security events.

This range of coverage includes systems whose compromise could result in the endangerment of public or employees health or safety, loss of public confidence, violation of regulatory requirements, loss or invalidation of proprietary or confidential information, environmental contamination, and/or economic loss or impact on an entity or on local or national security.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 62264-1, *Enterprise-control system integration – Part 1: Models and terminology*

ISO/IEC 15408-1, *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model*

3 Terms, definitions and abbreviations

3.1 General

Wherever possible, definitions have been adapted from those used in established industry sources. Some definitions have been adapted from more generic definitions used in the IT industry.

3.2 Terms and definitions

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

3.2.1

access

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

NOTE 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).

3.2.2

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 [10]³

[RFC 2828, modified]

³ Numbers in square brackets refer to the Bibliography.

3.2.3**accountability**

property of a system (including all of its system resources) that ensures that the actions of a system entity may be traced uniquely to that entity, which can be held responsible for its actions [10]

3.2.4**application**

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

3.2.5**area**

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

NOTE An area may contain manufacturing lines, process cells, and production units. Areas may be connected to each other by a site local area network and may contain systems related to the operations performed in that area.

3.2.6**asset**

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

NOTE In the case of industrial automation and control systems the physical assets that have the largest directly measurable value may be the equipment under control.

3.2.7**association**

cooperative relationship between system entities, usually for the purpose of transferring information between them [10]

3.2.8**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

3.2.9**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 [10]

NOTE There are different commonly recognized classes of attack:

- An "active attack" attempts to alter system resources or affect their operation.
- A "passive attack" attempts to learn or make use of information from the system but does not affect system resources.
- An "inside attack" is an attack initiated by an entity inside the security perimeter (an "insider") – 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.
- An "outside attack" is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (including an insider attacking from outside the security perimeter). Potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments.

3.2.10**attack tree**

formal, methodical way of finding ways to attack the security of a system

3.2.11

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 (see 3.2.100)

NOTE There are three forms of audit

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

3.2.12

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

3.2.13

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

3.2.14

authorization

right or permission that is granted to a system entity to access a system resource [10]

3.2.15

automated vehicle

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

3.2.16

availability (performance)

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 This ability depends on the combined aspects of the reliability performance, the maintainability performance and the maintenance support performance.

NOTE 2 Required external resources, other than maintenance resources do not affect the availability performance of the item.

NOTE 3 In French the term "disponibilité" is also used in the sense of "instantaneous availability".

3.2.17

border

edge or boundary of a physical or logical security zone

3.2.18

botnet

collection of software robots, or bots, which run autonomously

NOTE A botnet's originator can control the group remotely, possibly for nefarious purposes.

3.2.19

boundary

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

**3.2.20
channel**

specific communication link established within a communication conduit (see 3.2.27)

**3.2.21
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

**3.2.22
client**

device or application receiving or requesting services or information from a server application [11]

**3.2.23
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 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 media, and human interactions.

**3.2.24
communication security**

- a) 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
- b) state that is reached by applying security services, in particular, state of data confidentiality, integrity, and successfully authenticated communications entities [10]

NOTE 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.

**3.2.25
communication system**

arrangement of hardware, software, and propagation media to allow the transfer of messages from one application to another [9]

**3.2.26
compromise**

unauthorized disclosure, modification, substitution, or use of information (including plaintext cryptographic keys and other critical security parameters) [12]

**3.2.27
conduit**

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

NOTE This is analogous to the way that a physical conduit protects cables from physical damage.

**3.2.28
confidentiality**

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

3.2.29

control center

central location used to operate a set of assets

NOTE 1 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 In some industries the term "control room" may be more commonly used.

3.2.30

control equipment

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

NOTE The term also includes fieldbus networks where control logic and algorithms are executed on intelligent electronic devices that coordinate actions with each other, as well as systems used to monitor the process and the systems used to maintain the process.

3.2.31

control network

time-critical network that is typically connected to equipment that controls physical processes (see 3.2.97)

NOTE The control network can be subdivided into zones and there can be multiple separate control networks within one company or site.

3.2.32

cost

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

3.2.33

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 [10]

NOTE 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.

3.2.34

cryptographic algorithm

algorithm based upon the science of cryptography, including encryption algorithms, cryptographic hash algorithms, digital signature algorithms, and key agreement algorithms

3.2.35

cryptographic key

input parameter that varies the transformation performed by a cryptographic algorithm [10]

NOTE Usually shortened to "key".

3.2.36**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 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.

3.2.37**data confidentiality**

property that information is not made available or disclosed to any unauthorized system entity, including unauthorized individuals, entities, or processes [8]

3.2.38**data integrity**

property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner [10]

NOTE 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.

3.2.39**decryption**

process of changing cipher text into plaintext using a cryptographic algorithm and key (see 3.2.47) [10]

3.2.40**defence in depth**

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

NOTE 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.

3.2.41**demilitarized zone**

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

NOTE 1 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 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.

3.2.42**denial of service**

prevention or interruption of authorized access to a system resource or the delaying of system operations and functions [10]

NOTE 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.

3.2.43

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 [11]

3.2.44

distributed control system

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

NOTE 1 Distributed control systems may have shorter coupling time constants than those typically found in SCADA systems.

NOTE 2 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.

3.2.45

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 [10]

3.2.46

eavesdropping

monitoring or recording of communicated information by unauthorized parties

3.2.47

encryption

cryptographic transformation of plaintext into ciphertext that conceals the data's original meaning to prevent it from being known or used (see 3.2.39) [10]

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

3.2.48

enterprise

business entity that produces or transports products or operates and maintains infrastructure services

3.2.49

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)

3.2.50

equipment under control

equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities [13]

3.2.51

field I/O network

communications link (wired or wireless) that connects sensors and actuators to the control equipment

3.2.52

firewall

inter-network connection device that restricts data communication traffic between two connected networks [10]

NOTE A firewall may be either an application installed on a general-purpose computer or a dedicated platform (appliance) that forwards or rejects/drops packets on a network. Typically firewalls are used to define zone borders. Firewalls generally have rules restricting which ports are open.

3.2.53

gateway

relay mechanism that attaches to two (or more) computer networks that have similar functions but dissimilar implementations and that enables host computers on one network to communicate with hosts on the other [10]

NOTE Also described as an intermediate system that is the translation interface between two computer networks.

3.2.54

geographic site

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

NOTE 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.

3.2.55

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 [10]

3.2.56

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 [10]

3.2.57

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 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.

3.2.58

initial risk

risk before controls or countermeasures have been applied (see 3.2.87)

3.2.59

insider

trusted person, employee, contractor, or supplier who has information that is not generally known to the public (see 3.2.74)

3.2.60

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

3.2.61

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

3.2.62

interface

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

3.2.63

intrusion

unauthorized act of compromising a system (see 3.2.9)

3.2.64

intrusion detection

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

3.2.65

IP address

address of a computer or device that is assigned for identification and communication using the Internet Protocol and other protocols

3.2.66

ISO

International Organization for Standardization

NOTE ISO is not an acronym. The name derives from the Greek word iso, which means equal.

3.2.67

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 [10]

3.2.68

lines, units, cells

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

NOTE 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.

3.2.69

local area network

communications network designed to connect computers and other intelligent devices in a limited geographic area (typically less than 10 km) [9]

3.2.70**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 Malicious code attacks can take the form of viruses, worms, Trojan horses, or other automated exploits.

NOTE 2 Malicious code is also often referred to as “malware”.

3.2.71**manufacturing operations**

collection of production, maintenance, and quality assurance operations and their relationship to other activities of a production facility

NOTE Manufacturing operations include:

- manufacturing or processing facility activities that coordinate the personnel, equipment, and material involved in the conversion of raw materials or parts into products;
- functions that may be performed by physical equipment, human effort, and information systems;
- managing information about the schedules, use, capability, definition, history, and status of all resources (personnel, equipment, and material) within the manufacturing facility.

3.2.72**nonrepudiation**

security service that provides protection against false denial of involvement in a communication [10]

3.2.73**OPC**

set of specifications for the exchange of information in a process control environment

NOTE The abbreviation OPC originally came from “OLE for Process Control”, where OLE was the abbreviation for “Object Linking and Embedding”.

3.2.74**outsider**

person or group not trusted with inside access, who may or may not be known to the targeted organization (see 3.2.59)

NOTE Outsiders may or may not have been insiders at one time.

3.2.75**penetration**

successful unauthorized access to a protected system resource [10]

3.2.76**phishing**

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

3.2.77**plaintext**

unencoded data that is input to, and transformed by an encryption process, or that is output by a decryption process [10]

3.2.78**privilege**

authorization or set of authorizations to perform specific functions, especially in the context of a computer operating system [10]

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

3.2.79

process

series of operations performed in the making, treatment or transportation of a product or material

NOTE This technical specification makes extensive use of the term “process” to describe the equipment under control of the industrial automation and control system.

3.2.80

protocol

set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems [10]

3.2.81

reference model

structure that allows the modules and interfaces of a system to be described in a consistent manner

3.2.82

reliability

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

3.2.83

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 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.

3.2.84

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

3.2.85

repudiation

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

3.2.86

residual risk

remaining risk after the security controls or countermeasures have been applied

3.2.87

risk

expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence [10]

3.2.88

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 Types of resources include physical, logical and human.

NOTE 2 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.

3.2.89

risk management

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

3.2.90

risk mitigation controls

combination of countermeasures and business continuity plans

3.2.91

risk tolerance level

level of residual risk that is acceptable to an organization

3.2.92

role-based access control

form of identity-based access control where the system entities that are identified and controlled are functional positions in an organization or process [10]

3.2.93

router

gateway between two networks at OSI layer 3 that relays and directs data packets through an inter-network. The most common form of router passes Internet Protocol (IP) packets [10]

3.2.94

safety

freedom from unacceptable risk [3]

3.2.95

safety-instrumented system

system used to implement one or more safety-instrumented functions [3]

NOTE A safety-instrumented system is composed of any combination of sensor(s), logic solver(s), and actuator(s).

3.2.96

safety integrity level

discrete level (one out of four) for specifying the safety integrity requirements of the safety-instrumented functions to be allocated to the safety-instrumented systems [3]

NOTE Safety integrity level 4 has the highest level of safety integrity; safety integrity level 1 has the lowest.

3.2.97

safety network

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

3.2.98

secret

condition of information being protected from being known by any system entities except those intended to know it [10]

3.2.99 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 [10]
- 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 [13]
- e) prevention of illegal or unwanted penetration of, or interference with the proper and intended operation of an industrial automation and control system

NOTE 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).

3.2.100 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 [10]

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

3.2.101 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 [8]

3.2.102 security components

assets such as firewalls, authentication modules, or encryption software used to improve the security performance of an industrial automation and control system (see 3.2.33)

3.2.103 security control see 3.2.33

NOTE The term countermeasure has been chosen for this document to avoid confusion with the term "control" in the context of process control.

3.2.104 security event

occurrence in a system that is relevant to the security of the system [10]

3.2.105 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

3.2.106 security incident

adverse event in a system or network, or the threat of the occurrence of such an event [9]

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

3.2.107**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 [10]

3.2.108**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 [12]

3.2.109**security objective**

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

3.2.110**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 [10]

3.2.111**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 Tests, audits, tools, measures, or other methods are required to evaluate security practice performance.

3.2.112**security policy**

set of rules that specify or regulate how a system or organization provides security services to protect its assets [10]

3.2.113**security procedures**

definitions stating exactly how practices are implemented and executed

NOTE Security procedures are implemented through personnel training and actions using currently available and installed technology.

3.2.114**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

3.2.115**security services**

mechanisms used to provide confidentiality, data integrity, authentication, or non repudiation of information [10]