IEC/TS 62443-1-1

Edition 1.0 2009-07

TECHNICAL SPECIFICATION

colour inside

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

IEC/TS 62443-1-1:2009(E)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

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 corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub

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 It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC/TS 62443-1-1

Edition 1.0 2009-07

TECHNICAL SPECIFICATION

colour inside

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

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 networks[1], 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 62443-2-1[2] 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