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 It also gives information on projects, withdrawn and replaced publications.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

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 no repudiation of information [10]

3.2.116
security violation
act or event that disobeys or otherwise breaches security policy through an intrusion or the actions of a well-meaning insider

3.2.117
security zone
grouping of logical or physical assets that share common security requirements

NOTE 1 All unqualified uses of the term “zone” in this document should be assumed to refer to a security zone.

NOTE 2 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.

3.2.118
sensors and actuators
measuring or actuating elements connected to the process equipment and to the control system

3.2.119
server
device or application that provides information or services to client applications and devices [10]

3.2.120
sniffing
see 3.2.61

3.2.121
spoof
pretending to be an authorized user and performing an unauthorized action [10]

3.2.122
supervisory control and data acquisition system
SCADA system
type of loosely coupled distributed monitoring and control system commonly associated with electric power transmission and distribution systems, oil and gas pipelines, and water and sewage systems

NOTE Supervisory control systems are also used within batch, continuous, and discrete manufacturing plants to centralize monitoring and control activities for these sites.

3.2.123
system
interacting, interrelated, or interdependent elements forming a complex whole

3.2.124
system software
special software designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system and associated programs and data [11]

3.2.125
threat
potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm [10]

3.2.126
threat action
assault on system security [10]

3.2.127
threat agent
causative agent of a threat action

3.2.128
traffic analysis
inference of information from observable characteristics of data flow(s), even when the data are encrypted or otherwise not directly available, including the identities and locations of source(s) and destination(s) and the presence, amount, frequency, and duration of occurrence

3.2.129
Trojan horse
computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program [10]

3.2.130
trusted channel
communication link that can provide secure communication between security zones

3.2.131
untrusted channel
communication link that cannot provide secure communication between security zones

3.2.132
use case
technique for capturing potential functional requirements that employs the use of one or more scenarios that convey how the system should interact with the end user or another system to achieve a specific goal

NOTE Typically use cases treat the system as a black box, and the interactions with the system, including system responses, are as perceived from outside of the system. Use cases are popular because they simplify the description of requirements, and avoid the problem of making assumptions about how this functionality will be accomplished.

3.2.133
user
person, organization entity, or automated process that accesses a system, whether authorized to do so or not [10]

3.2.134
virus
self-replicating or self-reproducing program that spreads by inserting copies of itself into other executable code or documents

3.2.135
vulnerability
flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security policy [10]

3.2.136
wide area network
communications network designed to connect computers, networks and other devices over a large distance, such as across a country or the world [11]

3.2.137
wiretapping
attack that intercepts and accesses data and other information contained in a flow in a communication system [10]

NOTE 1 Although the term originally referred to making a mechanical connection to an electrical conductor that links two nodes, it is now used to refer to reading information from any sort of medium used for a link or even directly from a node, such as a gateway or sub-network switch.

NOTE 2 Active wiretapping attempts to alter the data or otherwise affects the flow while passive wiretapping only attempts to observe the flow and gain knowledge of information it contains.

3.2.138
worm
computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively [10]

3.2.139
zone
see 3.2.117

NOTE All unqualified uses of the term “zone” in this document should be assumed to refer to a security zone.

3.3 Abbreviations

This subclause defines the abbreviations used in this technical specification.

ANSI	American National Standards Institute
CIA	Confidentiality, Integrity and Availability
CN	Control Network
COTS	Commercial Off The Shelf
CSMS	Cyber Security Management System
DCS	Distributed Control System
DDoS	Distributed Denial of Service
DoS	Denial of Service
DMZ	Demilitarized Zone
FIPS	U. S. Federal Information Processing Standards
IACS	Industrial Automation and Control Systems
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
I/O	Input/Output
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
NASA	U. S. National Aeronautics and Space Administration
NOST	NASA Office of Standards and Technology
OSI	Open Systems Interconnect
PLC	Programmable Logic Controller
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SIL	Safety Integrity Level
SIS	Safety-Instrumented System
WAN	Wide Area Network

4 The situation

4.1 General

Industrial automation and control systems operate within a complex environment. Organizations are increasingly sharing information between business and industrial automation systems, and partners in one business venture may be competitors in another. However, because industrial automation and control systems equipment connect directly to a process, loss of trade secrets and interruption in the flow of information are not the only consequences of a security breach. The potential loss of life or production, environmental damage, regulatory violation, and compromise to operational safety are far more serious consequences. These may have ramifications beyond the targeted organization; they may grievously damage the infrastructure of the host region or nation.

External threats are not the only concern; knowledgeable insiders with malicious intent or even an innocent unintended act can pose a serious security risk. Additionally, industrial automation and control systems are often integrated with other business systems. Modifying or testing operational systems has led to unintended electronic effects on system operations. Personnel from outside the control systems area increasingly perform security testing on the systems, exacerbating the number and consequence of these effects. Combining all these factors, it is easy to see that the potential of someone gaining unauthorized or damaging access to an industrial process is not trivial.

Although technology changes and partner relationships may be good for business, they increase the potential risk of compromising security. As the threats to businesses increase, so does the need for security.

4.2 Current systems

Industrial automation and control systems have evolved from individual, isolated computers with proprietary operating systems and networks to interconnected systems and applications employing commercial off the shelf (COTS) technology (i.e., operating systems and protocols). These systems are now being integrated with enterprise systems and other business applications through various communication networks. This increased level of integration provides significant business benefits, including the following:

a) increased visibility of industrial control system activities (work in process, equipment status, production schedules) and integrated processing systems from the business level, contributing to the improved ability to conduct analyses to drive down production costs and improve productivity;

b) integrated manufacturing and production systems that have more direct access to business level information, enabling a more responsive enterprise;

c) common interfaces that reduce overall support costs and permit remote support of production processes;

d) remote monitoring of the process control systems that reduces support costs and allows problems to be solved more quickly.

It is possible to define standards for models, terms, and information exchanges that allow the industrial automation and control systems community to share information in a consistent way. However, this ability to exchange information increases vulnerability to misuse and attack by individuals with malicious intent and introduces potential risks to the enterprise using industrial automation and control systems.

Industrial automation and control systems' configurations can be very complex in terms of physical hardware, programming, and communications. This complexity can often make it difficult to determine the following points:

- who is authorized to access electronic information;
- when a user can have access to the information;

- what data or functions a user should be able to access;
- where the access request originates;
- how the access is requested.

4.3 Current trends

Several trends contribute to the increased emphasis on the security of industrial automation and control systems:

a) In recent years there has been a marked increase in malicious code attacks on business and personal computer systems. Businesses have reported more unauthorized attempts (either intentional or unintentional) to access electronic information each year than in the previous year.

b) Industrial automation and control systems are moving toward COTS operating systems and protocols and are interconnecting with business networks. This is making these systems susceptible to the same software attacks as those present in business and desktop devices.

c) Tools to automate attacks are commonly available on the Internet. The external threat from the use of these tools now includes cybercriminals and cyberterrorists who may have more resources and knowledge to attack an industrial automation and control system.

d) The use of joint ventures, alliance partners, and outsourced services in the industrial sector has led to a more complex situation with respect to the number of organizations and groups contributing to security of the industrial automation and control system. These practices need to be taken into account when developing security for these systems.

e) The focus on unauthorized access has broadened from amateur attackers or disgruntled employees to deliberate criminal or terrorist activities aimed at impacting large groups and facilities.

f) The adoption of industry document protocols such as Internet Protocol (IP) for communication between industrial automation and control systems and field devices. Implementing IP exposes these systems to the same vulnerabilities as business systems at the network layer.

These trends have combined to significantly increase organizations' risks associated with the design and operation of their industrial automation and control systems. At the same time, cybersecurity of industrial control systems has become a more significant and widely acknowledged concern. This shift requires more structured guidelines and procedures to define cybersecurity applicable to industrial automation and control systems, as well as the respective connectivity to other systems.

4.4 Potential impact

People who know the features of open operating systems and networks could potentially intrude into console devices, remote devices, databases, and, in some cases, control platforms. The effect of intruders on industrial automation and control systems may include the following:

a) unauthorized access, theft, or misuse of confidential information;

b) publication of information to unauthorized destinations;

c) loss of integrity or reliability of process data and production information;

d) loss of system availability;

e) process upsets leading to compromised process functionality, inferior product quality, lost production capacity, compromised process safety, or environmental releases;

f) equipment damage;

g) personal injury;

h) violation of legal and regulatory requirements;

i) risk to public health and confidence;

j) threat to a nation's security.

5 Concepts

5.1 General

This clause describes several underlying concepts that form the basis for the following clauses and for other standards in the IEC 62443 series. Specifically, it addresses questions such as:

a) What are the major concepts that are used to describe security?

b) What are the important concepts that form the basis for a comprehensive security program?

5.2 Security objectives

Information security has traditionally focused on achieving three objectives, confidentiality, integrity, and availability, which are often abbreviated by the acronym CIA. An information technology security strategy for typical back office or business systems may place the primary focus on confidentiality and the necessary access controls needed to achieve it. Integrity might fall to the second priority, with availability as the lowest.

In the industrial automation and control systems' environment, the general priority of these objectives is often different. Security in these systems is primarily concerned with maintaining the availability of all systems' components. There are inherent risks associated with industrial machinery that is controlled, monitored, or otherwise affected by industrial automation and control systems. Therefore, integrity is often second in importance. Usually confidentiality is of lesser importance, because often the data is raw in form and need to be analyzed within context to have any value.

The facet of time responsiveness is significant. Control systems can have requirements of system responsiveness in the one millisecond range, whereas traditional business systems are able to successfully operate with single or multiple second response times.

In some situations the priorities are completely inverted, as shown in Figure 1.

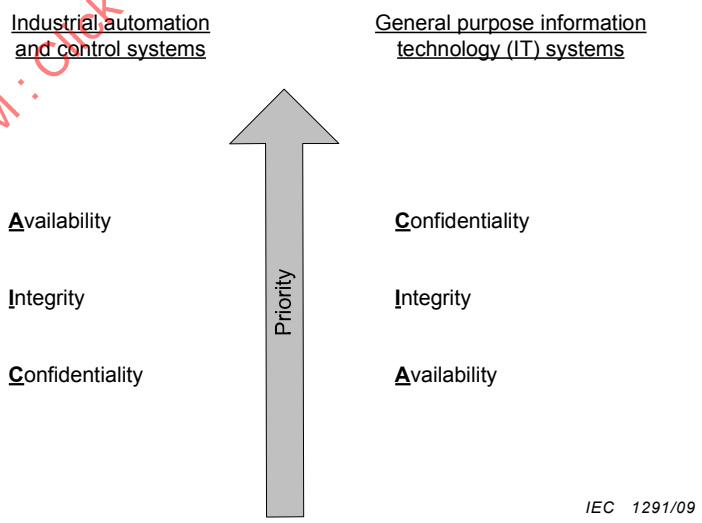

Figure 1 – Comparison of objectives between IACS and general IT systems

Depending on the circumstances, the integrity of the system could also have the highest priority. Certain operational requirements will cause individual components or the systems as a whole to have different priorities for the objectives (i.e., integrity or availability concerns may

outweigh confidentiality, or vice versa). This may in turn lead an organization to deploy different countermeasures to achieve these security objectives.

5.3 Foundational requirements

The simple CIA model shown in Figure 1 is not adequate for a full understanding of the requirements for security in industrial automation and control systems. Although it is beyond the scope of this technical specification to describe an exhaustive list of detailed requirements, there are several basic or foundational requirements that have been identified for industrial automation security. These are the following requirements:

a) Access Control (AC): control access to selected devices, information or both to protect against unauthorized interrogation of the device or information.

b) Use Control (UC): control use of selected devices, information or both to protect against unauthorized operation of the device or use of information.

c) Data Integrity (DI): ensure the integrity of data on selected communication channels to protect against unauthorized changes.

d) Data Confidentiality (DC): ensure the confidentiality of data on selected communication channels to protect against eavesdropping.

e) Restrict Data Flow (RDF): restrict the flow of data on communication channels to protect against the publication of information to unauthorized sources.

f) Timely Response to Event (TRE): respond to security violations by notifying the proper authority, reporting needed forensic evidence of the violation, and automatically taking timely corrective action in mission-critical or safety-critical situations.

g) Resource Availability (RA): ensure the availability of all network resources to protect against denial of service attacks.

All of these requirements are within the scope of this technical specification, although in some cases more detailed normative information will be provided by other standards in the IEC 62443 series. For example, technical requirements such as data integrity and data confidentiality will be addressed in detail in a future part of IEC 62443.

5.4 Defence in depth

It is typically not possible to achieve the security objectives through the use of a single countermeasure or technique. A superior approach is to use the concept of defence in depth, which involves applying multiple countermeasures in a layered or stepwise manner. For example, intrusion detection systems can be used to signal the penetration of a firewall.

5.5 Security context

The security context forms the basis for the interpretation of terminology and concepts and shows how the various elements of security relate to each other. The term security is considered here to mean the prevention of illegal or unwanted penetration of, or interference with, the proper and intended operation of an industrial automation and control system. Cybersecurity includes computer, network, or other programmable components of the system.

The context of security is based on the concepts of threats, risks, and countermeasures, as well as the relationships between them. The relationship between these concepts can be shown in a simple model. One such model, described in ISO/IEC 15408-1 (Common Criteria), is reproduced in Figure 2. A different view of the relationship is shown in Figure 3.

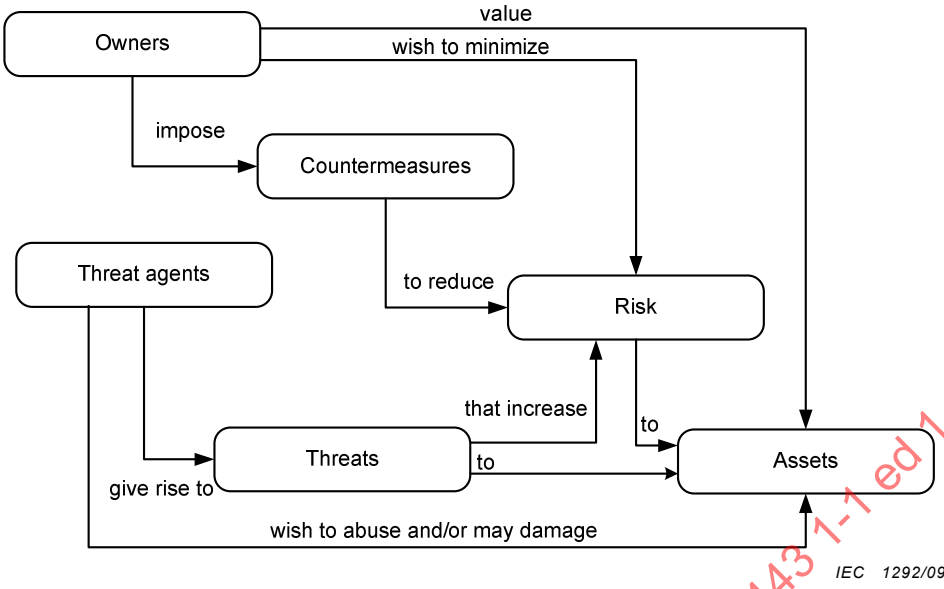

Figure 2 – Context element relationships

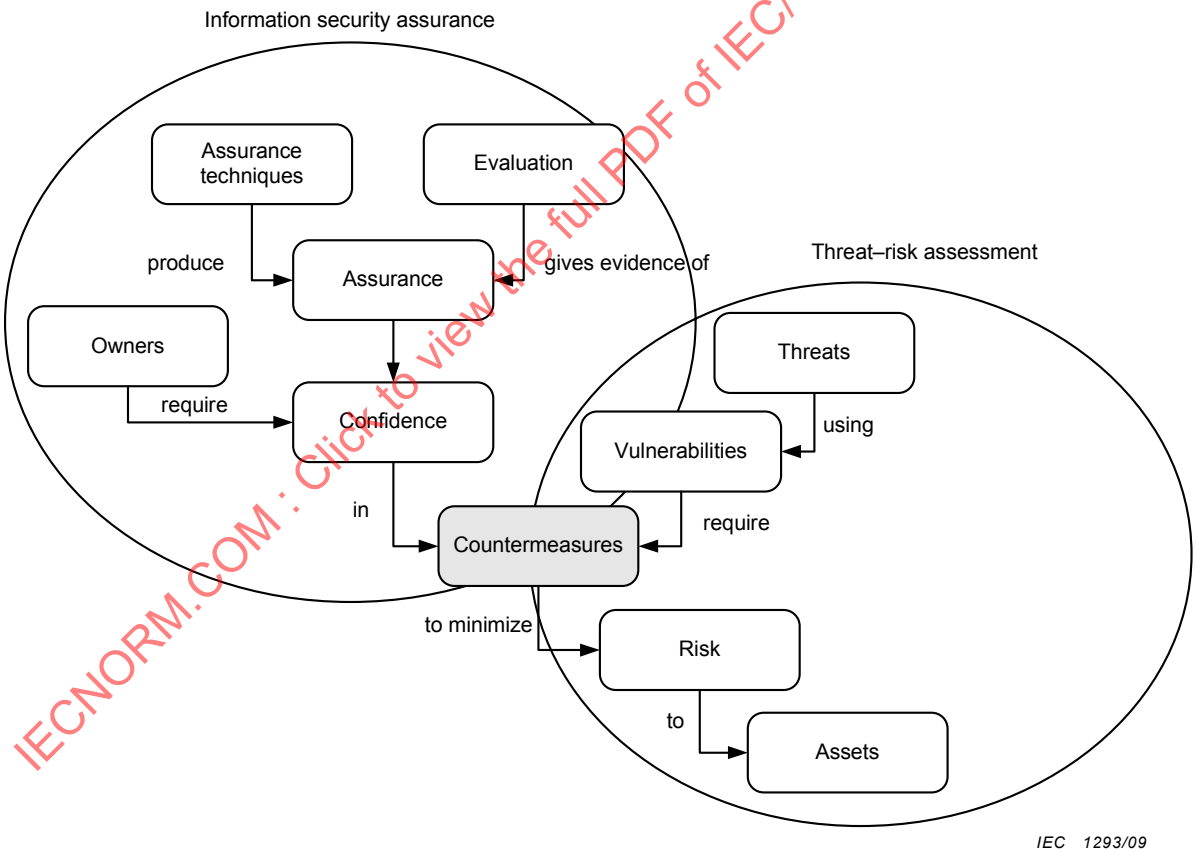

Figure 3 – Context model

The context model of Figure 3 shows how an expanded set of concepts is related within the two interconnected processes of information security assurance and threat-risk assessment.

5.6 Threat-risk assessment

5.6.1 General

Within the threat-risk assessment process, assets are subject to risks. These risks are in turn minimized through the use of countermeasures, which are applied to address vulnerabilities that are used or exploited by various threats. Each of these elements is described in more detail in the following subclauses.

5.6.2 Assets

5.6.2.1 Overview

Assets are the focus of a security program. They are what is being protected. In order to fully understand the risk to an IACS environment, it is first necessary to create an inventory of the assets that require protection. Assets may be classified as physical, logical or human.

a) Physical assets: physical assets include any physical component or group of components belonging to an organization. In the industrial environment, these may include control systems, physical network components and transmission media, conveyance systems, walls, rooms, buildings, material, or any other physical objects that are in any way involved with the control, monitoring, or analysis of production processes or in support of the general business. The most significant physical assets are those that make up the equipment that is under the control of the automation system.

b) Logical assets: logical assets are of an informational nature. They can include intellectual property, algorithms, proprietary practices, process-specific knowledge, or other informational elements that encapsulate an organization's ability to operate or innovate. Further, these types of assets can include public reputation, buyer confidence, or other measures that, if damaged, directly affect the business. Logical assets may be in the form of personal memory, documents, information contained on physical media, or electronic storage records dealing with the informational asset. Logical assets can also include test results, regulatory compliance data, or any other information considered sensitive or proprietary, or that could either provide or yield a competitive advantage. Loss of logical assets often causes very long lasting and damaging effects to an organization.

   Process automation assets are a special form of logical assets. They contain the automation logic employed in executing the industrial process. These processes are highly dependent upon the repetitive or continuous execution of precisely defined events. Compromise of process assets could come through either physical (e.g., destruction of media) or nonphysical (e.g., unauthorized modification) means, and result in some sort of loss of integrity or availability to the process itself.

c) Human assets: human assets include people and the knowledge and skills that they possess associated with their production activities. They can include required certifications, equipment-specific knowledge, or other activities not included in the automated production processes or important skills needed during emergencies. Rarely are processing facilities completely automated and disruption of the operations carried out by people could have a major impact on production although the physical and logical systems remain relatively intact. For example, an erroneous plant alarm could cause personnel to initiate shutdown and plant evacuation although nothing was physically or logically disrupted in the industrial automation and control systems. Any accident or attack that injures a person would be considered as impacting a human asset.

5.6.2.2 Valuing assets

To meet the qualification of either a physical or logical asset, the object needs to be either owned by, or under the custodial duties of the organization. It also needs to have value to the organization. The value of the asset may be expressed in either qualitative or quantitative terms. Some organizations will also consider qualitative valuation to be adequate reasoning for expressing asset loss in the risk analysis process.

a) Quantitative valuation of assets: an asset given a quantitative valuation has a precise monetary loss associated with it. This could be in terms of cost of replacement, cost of lost

sales, or other monetary measures. Quantitative analysis requires a rigorous cost analysis to obtain a precise number, but does afford an organization a much clearer picture of the potential impact from a loss.

b) Qualitative valuation of assets: qualitative loss typically expresses a more abstract level of loss such as a percentage or a relative value such as low impact, high impact, or no impact. Many assets may only be analyzed in terms of qualitative loss. Initiating a risk assessment process may begin with a qualitative valuation of assets for documenting high-level risks and for justifying the business case for spending money on remediation to reduce a risk, and later be supported by a quantitative analysis for a detailed picture of risk exposure.

Value may be categorized by the type of loss incurred, either direct or indirect.

c) Direct loss: direct loss represents the cost of replacing the asset. For a physical asset, this could include the replacement cost for the device itself. Logical assets have comparatively low direct loss when compared with their utility value, because the medium used to store the asset is typically low cost.

d) Indirect loss: indirect loss represents any loss caused by the loss of the asset that the organization may realize. This could include losses related to process downtime, rework, or other production costs due to loss of the asset. Indirect losses for physical assets typically include downstream effects due to loss of the component. Indirect losses for logical assets are often great. They include loss of public confidence, loss of license to operate because of regulatory violation, and loss of competitive advantage from release of intellectual property (e.g., confidential process technology).

5.6.2.3 Categorization of loss

By combining the information on asset types and valuation, it is possible to show the types of losses for each type of asset. This is summarized in Table 1.

Table 1 – Types of loss by asset type

Asset type	Direct loss	Indirect loss	Qualitative or quantitative
Physical	Can be high direct loss, represented by the replacement cost for the asset. Direct loss comes from damage to physical assets as a result of loss of integrity or availability, and the interruption of precise sequencing or consistent nature of a process.	Downstream effects as a result of loss, including loss of control, loss or damage to other assets, and downtime losses.	Qualitative or quantitative, may begin with qualitative for high-level risks, and later be quantitative for greater precision.
Logical	Low direct loss, as the storage media are often cheap and easily replaceable.	High indirect loss, often due to loss of intellectual property, compromise of proprietary procedures, or violation of regulatory compliance. Indirect losses from equipment damage or material release can lead to downtime, rework, reengineering, or other efforts to restore control over the industrial process.	Mostly qualitative, but some downstream effects may be quantitative.

Asset type	Direct loss	Indirect loss	Qualitative or quantitative
Human	Low to medium direct loss depending upon the extent of the injury to the person. Minor injuries with short recovery times may have low direct loss impact to the company even though the injury may have lasting impact to the person who is injured.	Low to high indirect loss depending upon the extent of the injury and the criticality of the person to the process. Overtime costs and temporary replacement costs may vary considerably depending upon the recovery time of the individual. Permanent disabling injuries or death may have high indirect loss costs when social responsibility and potential litigation and awards are factored into the assessment.	Immediate qualitative impact on production followed by quantitative impact for recovery or replacement.

5.6.3 Vulnerabilities

In simple terms, vulnerabilities are inherent weaknesses in systems, components, or organizations.

Vulnerabilities may be the result of intentional design choices or may be accidental, resulting from the failure to understand the operational environment. They may also emerge as equipment ages and eventually becomes obsolete, which occurs in a shorter time than is typical for the underlying process or equipment under control. Vulnerabilities are not limited to the electronic or network systems. Understanding the interaction between physical (including human) and electronic vulnerabilities is critical to establishing effective industrial automation and control system security.

An industrial automation and control system that initially has limited vulnerability may become more vulnerable with situations such as changing environment, changing technology, system component failure, unavailability of component replacements, personnel turnover, and greater threat intelligence.

5.6.4 Risk

5.6.4.1 Overview

Risk is generally defined as an expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence. Risk is a function of threat, vulnerability, and consequence, where consequence is the negative impact the organization experiences due to the specific harm to the organization's asset or assets by the specific threat or vulnerability. The threat and vulnerability components can be expressed in terms of likelihood. Likelihood is the probability that a specific action will occur.

Asset owners should rank and include the cost of mitigation or cost to repair in their estimate of risk. They should also determine the appropriate countermeasures for mitigating the most security exposures for the least financial exposure.

Any sound risk assessment methodology should analyze all involved systems in a layered approach, starting with systems closest to the threat, and working inward. The basic risk assessment process consists of three steps:

1) assess initial risk;
2) implement risk mitigation countermeasures;
3) assess residual risk.

Steps 2 and 3 of this process are repeated as required in order to reduce the residual risk to an acceptable level. Specifically, the second step includes evaluating existing controls and

implementing plans to add remedial or additional countermeasures. A more detailed description of the process of determining risk will be provided in a future part of IEC 62443.

Typical risks considered include the following:

a) personnel safety risks such as death or injury;

b) process safety risks such as equipment damage or business interruption;

c) information security risks such as cost, legal violations, or loss of brand image;

d) environmental risk such as notice of violation, legal violations, or major impact;

e) business continuity risks such as business interruption.

5.6.4.2 Risk tolerance level

The output of a qualitative risk analysis will consist of a list of assets or scenarios with an overall likelihood and a consequence ranking. It is a management responsibility to determine the appropriate response to items based on these rankings. Some organizations accept relatively high levels of risk (such as aggressive growth companies), while some companies are inherently conservative in terms of being risk adverse. Therefore, a certain level of residual risk may be acceptable to one organization and not to another. Even within the same company, individual plants may exhibit different risk appetites or tolerances. Management should explicitly define and understand what its risk appetite or tolerance is, so it can better analyze its level of response to residual risks identified.

Addressing the security of industrial automation and control systems does not, in general, introduce new risks, but it may contribute to a different perspective on the existing risks. For example, risks related to safety are typically given more attention in an industrial automation context.

Industrial automation and control systems security does not need to reinvent a process for defining the risk tolerance level; it is simply derived from other risk management practices in the organization.

5.6.4.3 Risk response

There are several potential responses to risk. Organizations can take some combination of actions in each situation, depending on the circumstances.

a) Design the risk out: one form of mitigation is to change the design of the system so the risk is removed. Some risks exist simply because access is available to something to which no access is ever needed. Completely disabling the unnecessary function or welding the function from access can mitigate the risk. Organizations can make the appropriate business decisions so the risk is not taken. This response may involve saying no to something, whether a new vendor product, system, or relationship.

b) Reduce the risk: risks can be decreased to an acceptable level through the implementation of countermeasures that reduce the likelihood or consequence of an attack. The key here is to achieve a level of good enough security, not to eliminate the risk.

c) Accept the risk: there is always an option to accept the risk, to see it as the cost of doing business. Organizations need to take some risks, and they cannot always be cost effectively mitigated or transferred.

d) Transfer or share the risk: it may be possible to establish some sort of insurance or agreement that transfers some or all of the risk to a third entity. A typical example of this is outsourcing of specific functions or services. This approach cannot always be effective, because it may not always cover all assets completely. A cybersecurity policy can recover certain damages, but not logical assets such as loss of customer confidence.

e) Eliminate or redesign redundant or ineffective controls: a good risk assessment process will identify these types of controls that need to be addressed so that more attention can be focused on controls that are effective and efficient.

5.6.5 Threats

5.6.5.1 Overview

Threats describe the possible actions that can be taken against a system. They come in many different forms, but two of the more common forms are:

a) Accidental: someone unfamiliar with proper procedure and policy or an honest oversight causes an accidental risk. It is also likely that an organization does not know all the risks and may uncover them by accident as it operates complex industrial automation and control systems.

b) Non-validated changes: updates, corrections, and other changes to operating systems, application programs, configurations, connectivity, and equipment can provide an unexpected security threat to the industrial automation and control systems or the respective production.

Threat agent is the term used to describe the entity that presents a threat. They are also known as adversaries or attackers. Threat agents come in many different forms. Examples include:

c) Insider: an insider is a trusted person, employee, contractor, or supplier who has information that is not generally known to the public. An insider can present a threat even if there is no intent to do harm. For example, the threat may arise as a result of an insider bypassing security controls to get the job done.

d) Outsider: an outsider is a person or group not trusted with inside access, which may or may not be known to the targeted organization. Outsiders may or may not have been insiders at one time.

e) Natural: natural events include storms, earthquakes, floods, and tornadoes, and are generally considered a physical threat.

Threats that become action are known as attacks (sometimes referred to as an intrusion). Whether designing components and systems or implementing a security program within a site or organization, it is possible to model attacks in order to ensure that countermeasures are in place to identify and deter them. Case modelling and attack trees are examples of methods that can be used.

Threats may be either passive or active. Each type is described in the following subclauses.

5.6.5.2 Passive threats

Passive information gathering can provide a potential intruder with valuable information. Threat agents usually gather passive information by casual verbal communications with employees and contractors. However, persons inside or outside the facilities can also gather passive information with visual observations. Passive information gathering could include data about shift changes, equipment operation, supply logistics, patrol schedules, and other vulnerabilities. Passive information gathering may be difficult to detect, especially when information is gathered in small increments from several sources. Maintaining observation for unusually curious persons, photographers, and personnel often outside their areas of responsibility can help organizations recognize passive information gathering, especially when combined with accurate background check information.

Sniffing is an example of a passive threat. It is the act of monitoring data in a communication stream. Wiretapping, intercepting data contained in a flow of information, is the most widely known means of sniffing. Sniffing can be very sophisticated. Tools are publicly available to sniff data on various communication networks. Although these devices are commonly used for configuration management, troubleshooting networks, and analyzing data traffic, they can also be used to gather specific data about any transaction occurring across the network. For example, in packet sniffing and password sniffing, the attacker secretly attaches to the network at a remote switch or computer. The sniffing tool then passively monitors the information sent through the network and captures the information to a disk that can later be downloaded and analyzed to obtain user's identifications and passwords.

5.6.5.3 Active threats

5.6.5.3.1 General

Active threats come in various forms, as described in the following subclauses.

5.6.5.3.2 Communication

The intent of a communication attack is to disrupt communications for an industrial automation and control system. Communication attacks can occur in several forms. They may occur at several levels within the system from the computer processor layer up and from outside the enterprise, as in a denial-of-service attack on communications systems.

5.6.5.3.3 Database injection

An injection is a form of attack on a database-driven website in which the attacker executes unauthorized commands by taking advantage of an insecure code on a system connected to the internet, bypassing the firewall. Injection attacks are used to steal information from a database from which the data would normally not be available and/or to gain access to an organization's host computers through the computer that is hosting the database.

5.6.5.3.4 Replay

Signals may be captured from control system communications paths and replayed later to provide access to secured systems or to falsify data in the industrial automation and control system. Potential intruders can replay access control signals, biometric signals, and other system signals to gain unauthorized access to secured areas or systems, hide illegitimate activities, or provide false distractions. A system might combine multiple paths for data acquisition, signaling, and control to prevent a single tap from gathering replay information for an entire subsystem, piece of equipment, application, or database.

5.6.5.3.5 Spoofing and impersonation

In networking, these terms are used to describe a variety of ways in which hardware and software can be fooled. Attackers can forge an e-mail header to make it appear as if the message came from somewhere or someone other than the actual source. IP spoofing, for example, involves trickery that makes a message appear as if it came from an authorized IP address.

5.6.5.3.6 Social engineering

Threat agents also obtain or attempt to obtain otherwise secure data by tricking an individual into revealing secure information. Social engineering is successful because its victims innately want to trust other people and are naturally helpful. The victims of social engineering are tricked into releasing information that they do not realize will be used to attack a computer network.

5.6.5.3.7 Phishing

This is a 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. Phishing relies on social engineering in that humans tend to believe in the security of a brand name, associating it with trustworthiness.

5.6.5.3.8 Malicious code

The purpose of a malicious code may be to gather information about systems or users, destroy system data, provide a foothold for further intrusion into the system, falsify system data and reports, or provide time-consuming irritation to system operations and maintenance personnel. Malicious code attacks can take the form of viruses, worms, automated exploits, or Trojan horses.

A virus is a program or piece of code inside another program that is loaded onto a computer without the user's knowledge and that runs against their wishes. Viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous, because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

An automated exploit code is placed into the system to gather information or notify someone or other systems when specific events or transactions occur. A relatively simple exploit code can gather information for future intrusions, financial exploitation, or statistical purposes (marketing). An automated exploit code can use other resources or applications already within the system to enhance its capabilities to gather information or destroy data. A fully automated exploit code is usually called a worm. A worm is a self-contained program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down.

A Trojan horse is a destructive program that masquerades as a benign application. Unlike viruses, Trojan horses (also known as "Trojans") do not replicate themselves, but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid a computer of viruses, but instead introduces viruses onto the computer.

A malicious code can be delivered in the form of a botnet, defined as a collection of compromised machines running programs under a common command and control infrastructure. A botnet's originator can control the group remotely, usually for nefarious purposes.

5.6.5.3.9 Denial of service

Denial (or degradation) of service attacks affects the availability of a network, operating system, or application resources. A popular form of network-based denial of service is the distributed denial of service (DDoS) attack, which leverages multiple compromised devices to cause significant damage to a network, device, or application.

5.6.5.3.10 Escalation of privileges

To mount an effective attack against a system, it is often necessary for threat agents to first obtain privileged access. With these increased privileges the attacker can take actions that would otherwise be prevented.

5.6.5.3.11 Physical destruction

Physical destruction attacks are aimed at destroying or incapacitating physical components (i.e., hardware, software storage devices, connections, sensors, and controllers) that are part of the industrial automation and control system. These attacks can come in the form of a physical attack on the components themselves or through a cyberattack that causes the system to perform actions that lead to physical damage, destruction, or incapacitation of the component.

5.6.6 Countermeasures

Countermeasures are actions taken, or provisions made for the purpose of reducing risk to an acceptable level, or to meet security policies. They do not typically eliminate risk. The nature of the countermeasures employed depends on the nature of the threat being addressed.

There are several possible countermeasures to address external threats. Examples include the following:

a) authentication of users and/or computers;

b) access controls;

c) intrusion detection;

d) encryption;

e) digital signatures;

f) resource isolation or segregation;

g) scanning for malicious software;

h) system activity monitoring;

i) physical security.

In the case of internal threats, a different approach may be required, since the attacker may have the ability to bypass some of the normal countermeasures such as access control. This makes it necessary to place more emphasis on countermeasures such as written policies, separation of duties, activity monitoring, system auditing and encryption.

Passive threats such as sniffing are very difficult to detect, because the sniffing tool only reads the information moving across the connected media and does not provide signals into the signaling path. Hard-connected sniffing can be detected with modern communication control devices, such as intelligent data network switches, but wireless sniffing is nearly impossible to detect even with very sophisticated and expensive radio telecommunications equipment. Sniffing access can be reduced by controlling and closing unused voice and data ports in the plant and by providing intelligence in communication control equipment.

5.7 Security program maturity

5.7.1 Overview

Driven by increasing cybersecurity risks, many organizations have taken a proactive approach towards addressing the security risks of their information technology systems and networks. They are beginning to realize that addressing cybersecurity is a continuous activity or process and not a project with an identified start and stop.

Historically, organizations providing and supporting business information systems and industrial automation and control systems operated in two mutually exclusive areas. The expertise and requirements of each organization were not understood or appreciated by the other. Issues arose as organizations tried to employ common IT security practices to industrial automation and control systems.

In some cases, the security practices were in opposition to normal production practices designed to maximize safety and continuity of production. Because today's open information technologies are used extensively in industrial automation and control systems, additional knowledge is required to safely employ these technologies. The IT and manufacturing or production organizations should work together and bring their knowledge and skills together to tackle security issues. In industries with a high potential for health, safety, and environmental incidents, it is important to involve Process Safety Management (PSM) and physical security personnel as well.

The goal is a mature security program that integrates all aspects of cybersecurity, incorporating desktop and business computing systems with industrial automation and control systems. Figure 4 shows the integration journey many businesses face. Many organizations have fairly detailed and complete cybersecurity programs for their business computer systems, but cybersecurity management practices are not as fully developed for IACS.

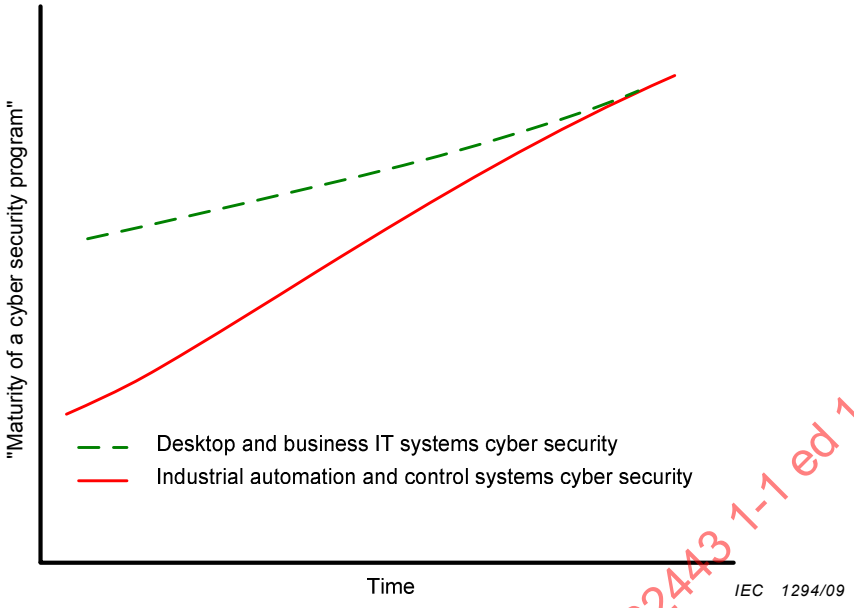

Figure 4 – Integration of business and IACS cybersecurity

A common mistake is to address cybersecurity as a project with a start-and end date. When this occurs, the security level often declines over time as is depicted in Figure 5. Cybersecurity risks constantly change as new threats and vulnerabilities surface along with ever-changing technology implementations. A different approach is needed to sustain the security gains and hold risk to an acceptable level.

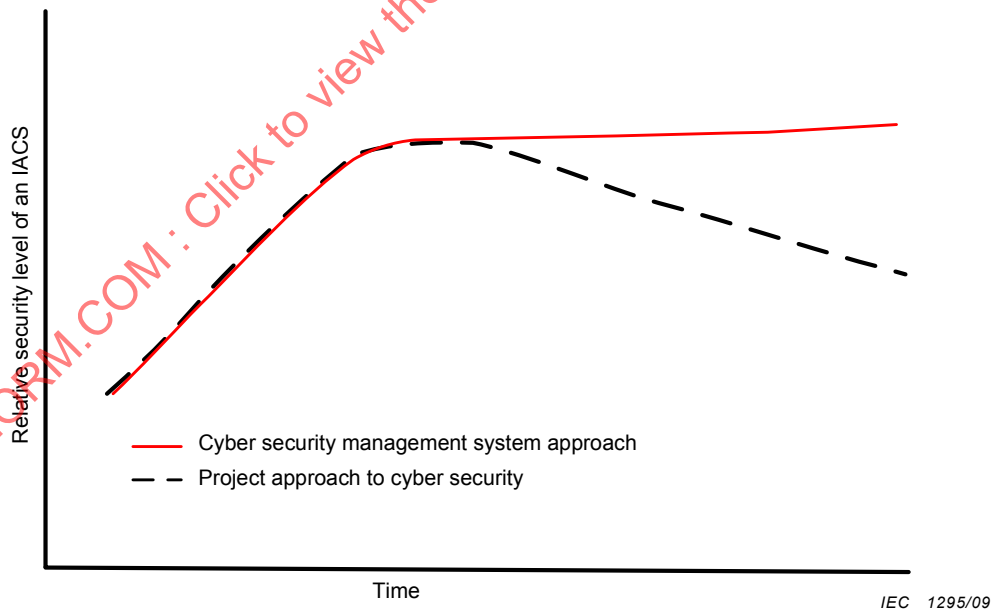

Figure 5 – Cybersecurity level over time

The recommendation is to develop and implement an organization-wide cybersecurity management system (CSMS) that includes program elements to reassess risk and take corrective actions to eliminate the tendency for security levels to decline over time. An in-depth description of the key elements of a cybersecurity management system is provided in the second document in this series. [8]

Every organization's journey to implement a cybersecurity management system will be different based on the organization's objectives and tolerance for risk. Integrating cybersecurity into an organization's document practices is a cultural change that takes time and resources. As the figures suggests, it cannot be achieved in one step. It is an evolutionary process that standardizes on the approach to cybersecurity. The security practices to be implemented should be proportionate to the risk level and will vary from one organization to another, and may even be different for various operations within the same organization based on global needs and requirements. Individual policies and procedures may also be different for each class of system within an organization because the level of risk and security requirements may be different. A cybersecurity management system establishes the overall program that accommodates these differences.

Education and awareness are critical for successfully addressing IACS cybersecurity risks as noted above. There are several options to consider:

a) Training the IACS personnel to understand the current information technology and cybersecurity issues.

b) Training IT personnel to understand IACS technologies, along with the process safety management processes and methods.

c) Developing practices that join the skill sets of all the organizations to deal with cybersecurity collaboratively.

For the cybersecurity program to be successful, it is necessary to assemble the right mix of people on both the mitigation projects and the overall CSMS program development. Figure 6 illustrates a typical range of skills and understanding that should be pulled together from multiple groups of people to reach the desired integrated, mature cybersecurity program state.

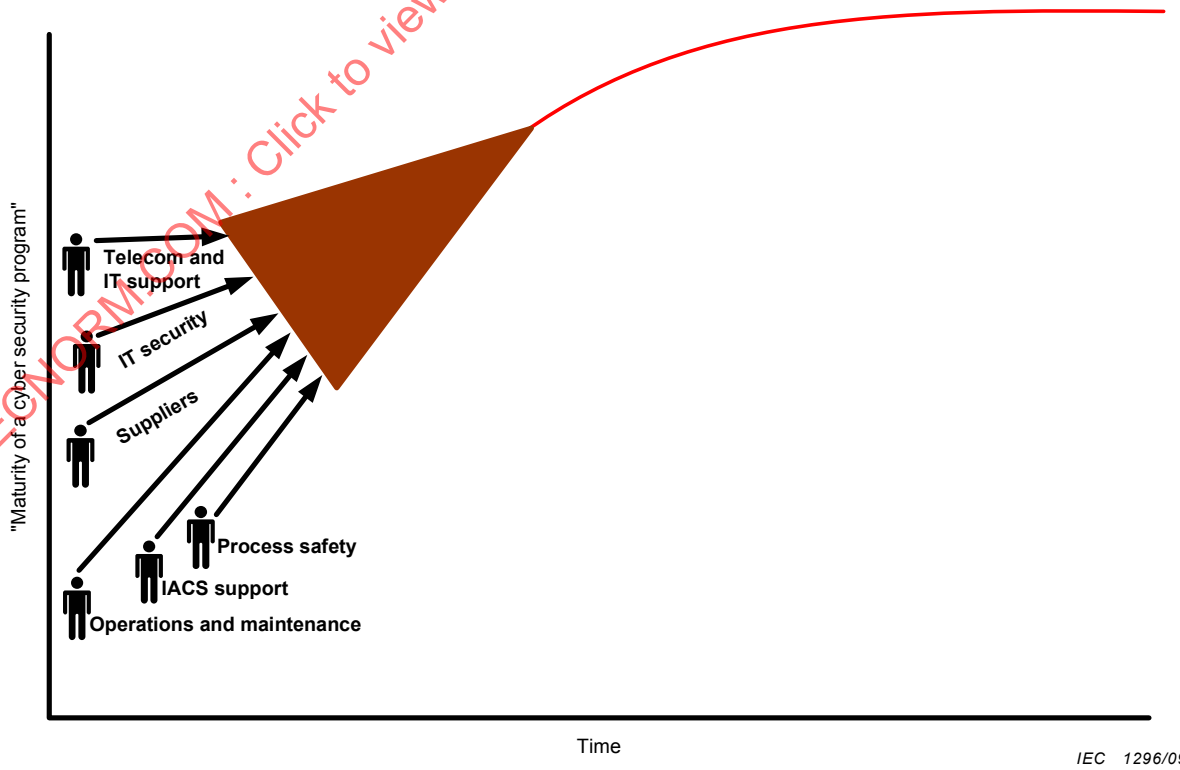

Figure 6 – Integration of resources to develop the CSMS

5.7.2 Maturity phases

It is possible to describe the relative maturity of a cybersecurity program in terms of a life cycle that consists of several phases. Each of these phases consists of one or more steps.

Portions of the industrial automation and control system, or control zones within a control system can be at different phases of maturity. There are several reasons for this situation, including budgetary constraints, vulnerability and threat assessments, schedules placed against risk analysis results, automation upgrades, plans for dissolution or replacement, plans to sell a segment of the facility or business, or availability of other resources to upgrade the security systems to a more mature phase.

Organizations can achieve a more detailed evaluation of security maturity by assessing achievements within portions of the industrial automation and control system in terms of the phases and steps shown in Table 2.

Table 2 – Security maturity phases

Phase	Step
Concept	Identification
	Concept
Functional analysis	Definition
Implementation	Functional design
	Detailed design
	Construction
Operations	Operations
	Compliance monitoring
Recycle and disposal	Disposal
	Dissolution

Table 3 through Table 7 provide general descriptions for each of the phases and steps in the maturity of a life cycle.

Table 3 – Concept phase

Step	Description
Identification	Recognize need for protection of property, assets, services, or personnel
	Start developing the security program
Concept	Continue developing the security program
	Document assets, services, and personnel needing some level of protection
	Document potential internal and external threats to the enterprise
	Establish security mission, visions, and values
	Develop security policies for industrial automation and control systems and equipment, information systems and personnel

Table 4 – Functional analysis phase

Step	Description
Definition	Continue developing the security program
	Establish security functional requirements for industrial automation and control systems and equipment, production systems, information systems, and personnel
	Perform vulnerability assessment of facilities and associated services against the list of potential threats
	Discover and determine legal requirements for industrial automation and control systems
	Perform a risk analysis of potential vulnerabilities and threats
	Categorize risks, potential impacts to the enterprise, and potential mitigations
	Segment security work into controllable tasks and modules for development of functional designs
	Establish network functional definitions for security portions of industrial automation and control systems

Table 5 – Implementation phase

Step	Description
Functional design	Development of the security program is completed in this phase Define functional security requirements for enterprise zones, plant zones, and control zones. Potential activities and events are defined and documented to perform the functional requirements and implement plans for a secured enterprise Define functional security organization and structure Define functions required in the implementation plan Define and publish security zones, borders, and access control portals Complete and issue security policies, and procedures
Detailed design	Design physical and logical systems to perform the functional requirements previously defined for security Conduct training programs Implementation plan is fully developed Initiate asset management and change management programs Design borders and access control portals for protected zones
Construction	Implementation plan is executed. Physical security equipment, logical applications, configurations, personnel procedures are installed to complete the secured zones and borders within the enterprise. Access control portal attributes are activated and maintained Training programs are completed Asset management and change management programs are functional and operating Security system turnover packages are completed and ready for acceptance by operations and maintenance personnel

Table 6 – Operations phase

Step	Description
Operations	Security equipment, services, applications and configurations are completed and accepted by operations and maintenance Personnel are trained, and continued training is provided on security matters Maintenance monitors security portions of enterprise, plant, or control zones and keeps them functioning properly Asset management and change management is operational and maintained
Compliance monitoring	Internal audits Risk reviews External audits

Table 7 – Recycle and disposal phase

Step	Description
Disposal	Obsolete security systems are properly disassembled and disposed of Security borders are updated or recreated for zone protection Access control portals are created, redefined, reconfigured, or closed Personnel is briefed about changes in the security systems and items along with the impact to associated security systems
Dissolution	Intellectual property is properly collected, documented, and securely archived or destroyed Access control portals and respective links are closed Personnel are briefed about dissolution of the security systems and items along with the impact to remaining security systems

5.8 Policies

5.8.1 Overview

Security policies enable an organization to follow a consistent program for maintaining an acceptable level of security. Policies are defined at different levels in an organization, ranging from governance or management policies established at the enterprise level to operation policies defining the details of security administration. Policies at the most specific level are the organization's document against which security audits can measure compliance.

Security *policies* are the rules that specify or regulate how an organization protects sensitive and critical system resources. Policies unambiguously state what is mandatory. Because policies are mandatory and unambiguous, they make audits possible. The organization's security policies also take into account legal, regulatory, and contractual obligations. They are the measuring stick against which audits test the actual practices of the organization.

Complementing policies are *procedures*. Security procedures define in detail the sequence of steps necessary to provide a certain security measure. Because of their level of detail, procedures apply to a specific issue. They may pertain to a specific technology. Policies reference procedures and mandate their use.

Contrasting with policies and procedures are *guidelines*. Guidelines are not mandatory. They are intended to describe a way to do something that is desirable but not mandatory. Because guidelines are not mandatory and may be ambiguous, practices cannot be audited against guidelines. Guidelines are sometimes written by a group that does not have the authority to require them to be followed. Guidelines are inappropriate to describe practices that are mandatory.

Because the policies and procedures for different parts of an organization are often different, it is important that they be adequately coordinated. Specifically, the security policy for industrial automation and control systems should be coordinated with similar policies for general purpose IT security. The security program will work more successfully if there are good working relationships among the parties, and a well-coordinated set of policies can support good relationships.

Some consistency to the structure of the various policies and procedures increases the coherence of the overall set of policies and procedures. Each policy or procedure document has a short but precise statement of its purpose. It also has a statement of scope that defines where the document applies. It has a description of the risks that it is intended to reduce and of the key principles of the document. These common items guide the reader by providing more information about the intention of the policy or procedure. They also describe the intent of the document to provide guidance, which is useful when the document needs to be revised.

Different phases in a system's life cycle have different profiles of security issues. Security policies and procedures may address only certain life cycle phases. Some policies and procedures may specify that they only pertain to certain phases. All of the security concerns from all of the various phases are addressed in corresponding places in the set of security policies and procedures.

Security policies and procedures contain instructions on how the organization will measure compliance and update the policies. Organizations often recognize that policies need to be updated when performing or evaluating audits. Audits may identify ambiguities in policies and procedures as well as parts of policies and procedures that do not make the required process or outcome clear. Audits can identify issues that should be added to policies and procedures. Audits may also identify requirements that should be re-evaluated and adjusted or possibly retracted.

Policies and procedures should allow for unforeseen circumstances that make it infeasible to follow them. Policies should also state how to document and approve exceptions to policies and procedures. Documenting approved exceptions leads to a clearer state of security than leaving imprecision and ambiguity in the policies and procedures.

In addition, organizations should be unambiguous about what is a requirement versus what is optional advice in a policy. Precise use of verbs like shall, should, may and is, removes the ambiguity. Policy statements can define these words in their introduction sections to be more precise. "Shall" is used for requirements; "should" is used for recommendations. "May" is used for advice that is optional. It can be appropriate to provide options for addressing a requirement. Phrases like "when possible" or "unless necessary" introduce ambiguity unless the statement also describes how to determine whether the case is possible or necessary.

Policies and procedures identify who is responsible for what. Is the process-control staff responsible for the control network? Is it responsible for a demilitarized zone (DMZ) between the control network and the enterprise network? If a corporate information systems department is responsible for conditions that require the process-control staff to perform certain operations, then these operations should be described.

For an organization that is just starting to create its security program, policies and procedures are a good place to begin. Initially, they can be written to cover the set of security practices that the organization is equipped to handle in the near term. Over time they can be revised and tightened as the organization's capability grows. They can be put in place without the lead time of procuring and installing systems and devices.

5.8.2 Enterprise level policy

The policy at the enterprise level mandates the security program and sets the direction. It states the organization's overall security objectives.

The policy statement of top management should be circumspect enough to remain pertinent and accurate through changes in the structure of the organization, changes in system and security technology, and changes in the kinds of security threats. By being circumspect, the policy can be stable and will need to be rewritten only when the organization's basic position on security changes. However, the policy statement is also unambiguous; it clearly identifies what is required.

The enterprise level policy identifies areas of responsibility and assigns accountability for those areas. The policy can define the relationship between the IT department and plant operations and identify their different responsibilities. The policy can differentiate security objectives of the control system from those of the enterprise network. For example, maintaining confidentiality may be a top consideration of security for the enterprise network, whereas maintaining continuous operation may be a top consideration for the control system.

In addition, the policy identifies particular standards and regulations that apply to the organization. It may identify training as an important component of the security program. The policy may also indicate the consequences for policy violations.

Management should communicate the policy throughout the organization so that all employees understand it.

5.8.3 Operational policies and procedures

Operational policies and procedures are developed at lower levels of the organization to specify how the enterprise level policy is implemented in a specific set of circumstances. Security procedures put the policy into effect. They define what the organization will do to achieve the objectives and to meet the requirements of the policy. The procedures establish processes that will address all the concerns of the policy.

The procedures address all components needed in a security program, including the following:

a) system design;

b) procurement;

c) installation;

d) process operation;

e) system maintenance;

f) personnel;

g) audit;

h) training.

The procedures identify specific activities, who is accountable for their performance, and when activities will be performed.

The written procedures describe the process by which they will be changed when the situation changes. Each policy or procedure has an identified owner responsible for recognizing when updates are needed and for ensuring they are made.

The effectiveness of policies and procedures should be measured to check whether they serve their intended purpose. The cost to the organization should also be measured, so the organization can determine whether the balance of risk reduction aligns with the cost to implement the policies. If the balance is unacceptable, the policy and procedures may have to be adjusted. Procedures also have to be updated to reflect changes in technology.

Procedures are able to support audits. A security audit compares the observed actions of the organization against the written procedures.

5.8.4 Topics covered by policies and procedures

5.8.4.1 General

There are several topics that policies and procedures can cover. Every organization is different and should determine the appropriate policies and procedures that are applicable for its industrial automation and control systems. Possible topics include:

5.8.4.2 Risk management

Risk management is vital to developing a cost-effective security program that provides a uniform layer of adequate security, but that does not require equipment or procedures that are too costly and significantly beyond the range of adequate security. However, risk management is complex and needs to be tailored to the organization. The policy on risk management defines how an acceptable level of risk is determined and how to control the risk. This level

varies depending upon the goals and circumstances for a particular organization. The process for determining risk level should be repeated periodically in order to accommodate changes to the environment.

5.8.4.3 Access management

Security is improved in a system by restricting access to only those users who need and are trusted with the access. An access management policy identifies different roles of users and what kind of access each role needs to each class of asset (physical or logical). It specifies the responsibilities of employees to protect the assets and the responsibilities of administrators to maintain access management procedures. Authorization for these access privileges should have well-documented approval by management and be periodically reviewed. Access management may be as important or even more important to system integrity and availability as the need to protect data confidentiality.

5.8.4.4 Availability and continuity planning

Policies in this area provide the necessary framework and requirements expectations for backup and recovery, as well as business continuity and disaster recovery planning. They also define archiving characteristics (e.g., how long data should be retained).

5.8.4.5 Physical security

The security of the control system depends upon the physical security of the space that contains the control system. The plant site may already have a physical security policy before the security policy is written for the control system. However, policies related to systems' physical access may differ from those involving non-systems assets. For instance, all oil refinery personnel may have general access to almost all facilities within the plant fences, but IT infrastructure rooms may need to have access limited to only IT-related personnel – if for no other reason than to prevent accidental damage. The control system security policy should include a reference to the physical security policy and state its dependency. The security policy for the control system should contain enough specifics on physical security to make any specific application of the site physical security policy to the control system. For example, such a policy might state: "*some equipment shall be in locked cabinets, and the keys shall be kept in a restricted place.*"

5.8.4.6 Architecture

Policies and procedures describe secure configurations of control systems including such issues as the following:

a) recommended network designs;

b) recommended firewall configuration;

c) user authorization and authentication;

d) interconnecting different process control networks;

e) use of wireless communications;

f) domains and trust relationships;

g) patch management (including authentication);

h) anti-virus management;

i) system hardening in terms of closing software ports, disabling or avoiding unused or dangerous services, and disabling the use of removable storage devices;

j) access to external networks (i.e., the Internet);

k) appropriate use of e-mail.

5.8.4.7 Portable devices

Portable devices pose all the security risks of stationary equipment, but their mobility makes it less likely that they will be covered by the normal security procedures from installation to audit. Their portability provides additional opportunities for corruption while outside physical security zones or for interception of information while connecting to secure zones. Thus, a special policy is often needed to cover portable devices. The policy should require the same security protection as a stationary device, but the technical and administrative mechanisms that provide this protection may differ.

5.8.4.8 Wireless devices and sensors

Control equipment using radio frequency transmission in place of wires has been widely used in certain control system applications for many years. As costs decrease and new standards emerge, potential applications in automation and control systems continue to expand, in part due to lower installation costs. A key difference between wired and wireless devices is that in the latter case, signals are not confined within a physical security boundary, making them more prone to interception and corruption. Therefore, a security policy specific to wireless devices is appropriate for organizations that currently use or may in the future deploy wireless devices or sensors in their operations. The policy may specify which applications can use wireless devices, what protection and administrative methods are required, and how wired and wireless networks are interconnected.

5.8.4.9 Remote access

Remote access bypasses the local physical security controls of the boundaries of the system. It extends access to the trusted zone to a completely different geographic location and includes a computer that may not have undergone the security checks of the computers that are physically in the area of the trusted zone. Different mechanisms are required to provide the same level of security as the trusted zone.

5.8.4.10 Personnel

Personnel issues are likely to be defined in the enterprise personnel- and IT security policies. The control system security policy provides specifics, whereas the more general policies do not include control system aspects. For example, the control system security policies coordinate control system access roles with personnel screening and monitoring practices.

5.8.4.11 Subcontractor policy

Security issues include work that may involve subcontractors in roles such as supplier, integrator, maintenance service provider, or consultant. A security policy that covers subcontractors addresses the interactions with the subcontractor that could open vulnerabilities. The policy identifies the responsibilities of the different parties. It addresses the changing responsibilities as projects progress through their phases and as materials and systems are delivered. The policy may require certain terms to be written into contracts with subcontractors.

Without proper management of contract programmers, application integrity may be compromised or programming code may not be maintainable. It is important to find well-qualified contract programmers who will follow the organization's programming and documentation standards and perform adequate testing, as well as being trustworthy and timely.

5.8.4.12 Auditing

The security of the system is audited regularly to measure the degree of compliance with the security policies and practices. The security policy addresses the need for audits and specifies the responsibility, the regularity, and the requirement for corrective action. A comprehensive auditing process may address aspects other than security, such as process efficiency and effectiveness, and regulatory compliance.

5.8.4.13 Security policy updating

The security policy is monitored to determine changes needed in the policies themselves. Monitoring security policy is a part of each policy and procedure document, and the enterprise security policy sets forth the overall approach. Each operational policy and procedure document contains a statement of when and by whom the policy or procedure itself is to be reviewed and updated.

Training programs should be in place for new hires, operations, maintenance, upgrades and succession planning. Training programs should be well documented, structured, and updated at regular intervals to incorporate changes in the operating environment.

5.9 Security zones

5.9.1 General

Every situation has a different acceptable level of security. For large or complex systems it may not be practical or necessary to apply the same level of security to all components. Differences can be addressed by using the concept of a security *zone*, or area under protection. A security zone is a logical grouping of physical, informational, and application assets sharing common security requirements. This concept applies to the electronic environment where some systems are included in the security zone and all others are outside the zone. There can also be zones within zones, or subzones, that provide layered security, giving defence in depth and addressing multiple levels of security requirements. Defence in depth can also be accomplished by assigning different properties to security zones.

A security zone has a border, which is the boundary between included and excluded elements. The concept of a zone also implies the need to access the assets in a zone from both within and without. This defines the communication and access required to allow information and people to move within and between the security zones. Zones may be considered to be trusted or untrusted.

Security zones can be defined in either a physical sense (a physical zone) or in a logical manner (virtual zone). Physical zones are defined by grouping assets by physical location. In this type of zone it is easy to determine which assets are within each zone. Virtual zones are defined by grouping assets, or parts of physical assets, into security zones based on functionality or other characteristics, rather than the actual location of the assets.

5.9.2 Determining requirements

5.9.2.1 Overview

When defining a security zone, an organization should first assess the security requirements (security goals) and then determine whether a particular asset should be considered within the zone or outside the zone. The security requirements can be broken down into the following types:

5.9.2.2 Communications' access

For a group of assets within a security border to provide value, they need to be linked to assets outside the security zone. This access can be in many forms, including physical movement of assets (products) and people (employees and vendors) or electronic communication with entities outside the security zone.

Remote communication is the transfer of information to and from entities that are not in proximity to each other. For the purposes of this technical specification, remote access is defined as communication with assets that are outside the perimeter of the security zone being addressed.

Local access is usually considered as communication between assets within a single security zone.

5.9.2.3 Physical access and proximity

Physical security zones are used to limit access to a particular area because all the systems in that area require the same level of trust of their human operators, maintainers, and developers. This does not preclude having a higher-level physical security zone embedded within a lower-level physical security zone or a higher-level communication access zone within a lower-level physical security zone. For physical zones, locks on doors or other physical means protect against unauthorized access. The boundary is the wall or cabinet that restricts access. Physical zones should have physical boundaries commensurate with the level of security desired, and aligned with other asset security plans.

One example of a physical security zone is a typical manufacturing plant. Authorized people are allowed into the plant by an authorizing agent (security guard or ID), and unauthorized people are restricted from entering by the same authorizing agent and by fences.

Assets that are within the security border are those that need to be protected to a given security level, or policy. All devices that are within the border should share the same minimum level of security requirements. In other terms, they should be protected to meet the same security policy. Protection mechanisms can differ depending on the asset being protected.

Assets that are outside the security zone are by definition at a lesser or different security level. They are not protected to the same security level, and by definition cannot be trusted to the same security level or policy.

5.10 Conduits

5.10.1 General

Information needs to flow into, out of, and within a security zone. Even in a non-networked system, some communication exists (e.g., intermittent connection of programming devices to create and maintain the systems). To cover the security aspects of communication and to provide a construct to encompass the unique requirements of communications, this document is defining a special type of security zone: a communications' conduit.

A conduit is a particular type of security zone that groups communications that can be logically organized into a grouping of information flows within and also external to a zone. It can be a single service (i.e., a single Ethernet network) or can be made up of multiple data carriers (multiple network cables and direct physical accesses). As with zones, it can be made of both physical and logical constructs. Conduits may connect entities within a zone or may connect different zones.

As with zones, conduits may be either trusted or untrusted. Conduits that do not cross zone boundaries are typically trusted by the communicating processes within the zone. Trusted conduits crossing zone boundaries need to use an end-to-end secure process.

Untrusted conduits are those that are not at the same level of security as the zone endpoint. In this case the actual communication security becomes the responsibility of the individual channel. This is illustrated in Figure 7.

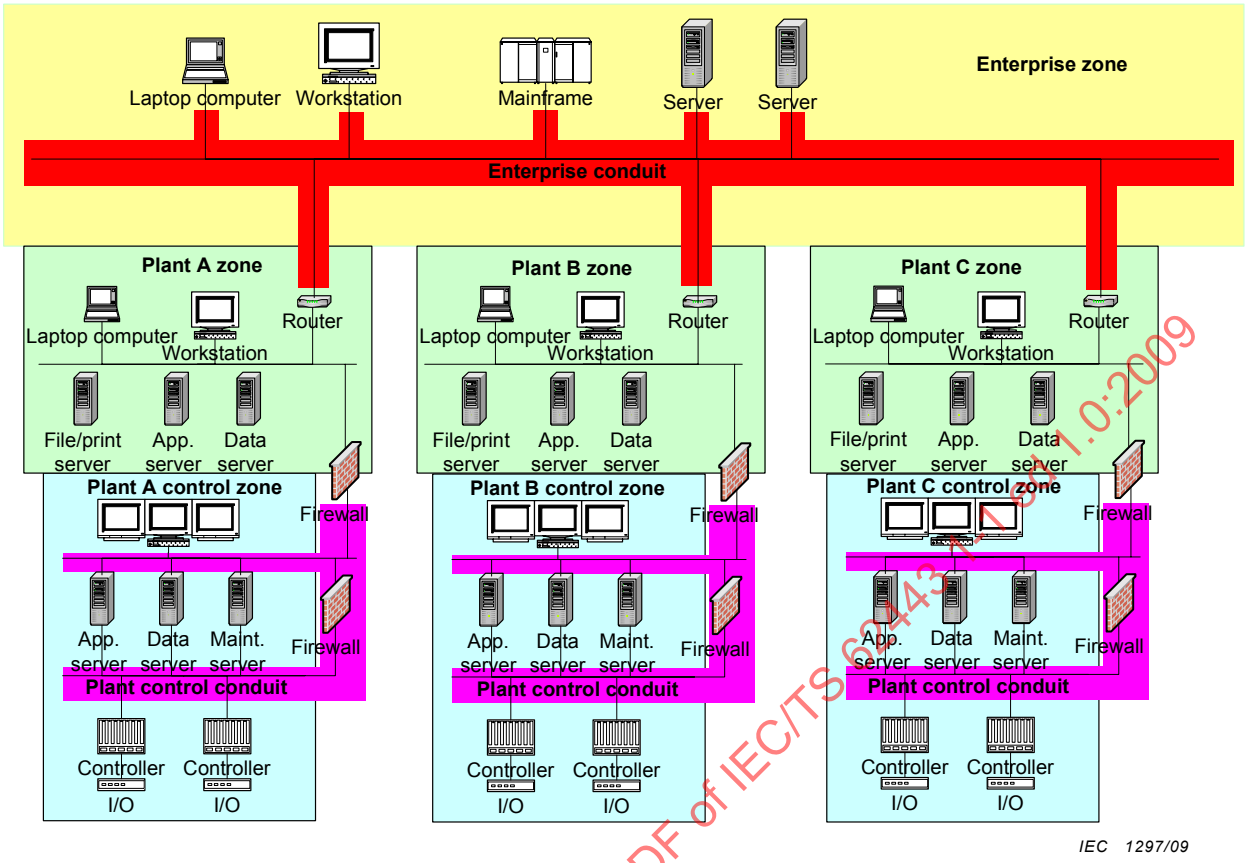

Figure 7 – Conduit example

Figure 7 represents a three-plant organization with separate corporate headquarters. The three plants are connected to the enterprise network to allow communications to headquarters and the other plants. Four possible conduits are defined in the drawing (others would also be defined, but are skipped for brevity). The first is the enterprise conduit, shown at the top of the figure. It connects multiple plants at different locations to the corporate data center. If the wide area network (WAN) is constructed using leased or private communications, then it could be considered a trusted conduit. If it uses both public and private networks, then it may be classified as untrusted. Included in the conduit are all of the communications' equipment and firewalls that make up the plant links.

Instances of the second conduit class are shown in each plant. Here each of the plants has its own trusted conduit to allow control communication.

5.10.2 Channels

Channels are the specific communication links established within a communication conduit. Channels inherit the security properties of the conduit used as the communication media (i.e., a channel within a secured conduit will maintain the security level of the secured conduit). Channels may be trusted or untrusted.

Trusted channels are communication links that allow secure communication with other security zones. A trusted channel can be used to extend a virtual security zone to include entities outside the physical security zone.

Untrusted channels are communication paths that are not at the same level of security as the security zone under study. The communications to and from the reference zone (the zone that defines the communication as non-secure) need to be validated before accepting the information.

5.11 Security levels

5.11.1 General

The security level concept has been created to focus thinking about security on a zone basis rather than on an individual device basis or system basis. Often an IACS consists of devices and systems from multiple vendors, all functioning together to provide the integrated automation functions for the industrial operation. Just as the functional capabilities of the individual devices contribute to the capability of the IACS, the security capabilities of the individual devices and implemented countermeasures need to function with each other to achieve a desired level of security for a zone. Security levels provide a frame of reference for making decisions on the use of countermeasures and devices with differing inherent security capabilities.

Security levels provide a qualitative approach to addressing security for a zone. As a qualitative method, security level definition has applicability for comparing and managing the security of zones within an organization. As more data becomes available and the mathematical representations of risk, threats, and security incidents are developed, this concept will move to a quantitative approach for selection and verification of Security Levels (SL). It will have applicability to both end user companies, and vendors of IACS and security products. It will be used to select IACS devices and countermeasures to be used within a zone and to identify and compare security of zones in different organizations across industry segments.

Each organization using the security level method should establish a definition of what each level represents and how to measure the level of security for the zone. This definition or characterization should be used consistently across the organization. The security level may be used to identify a comprehensive layered defence-in-depth strategy for a zone that includes hardware and software-based technical countermeasures along with administrative-type countermeasures.

Security level corresponds 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. The security level method provides the ability to categorize risk for a zone or conduit. It also helps define the required effectiveness of countermeasures used to prevent unauthorized electronic intervention that can read or impact the normal functioning of devices and systems within the zone or conduit. Security level is a property of a zone and conduit rather than of a device, system, or any part of a system.

A minimum of three security levels is recommended. The three levels can be qualitatively described as shown in Table 8. Organizations may choose to expand on this and define additional security levels to describe their unique security requirements.

Table 8 – Security levels

Security level	Qualitative description
1	Low
2	Medium
3	High

5.11.2 Types of security levels

5.11.2.1 General

Three different types of security levels can be defined as follows:

a) SL(target) - target security level for a zone or conduit;

b) SL(achieved) - achieved security level of a zone or conduit;

c) SL(capability) - security level capability of countermeasures associated with a zone or conduit or inherent security level capability of devices or systems within a zone or conduit.

5.11.2.2 SL(target) – target security level

A target security level should be assigned to a zone. A target security level may be assigned to a conduit. SL(target) for a zone and conduit is determined during risk assessment. It is not required to assign a target security level to conduits as long as the security properties associated with the conduit are taken into consideration during risk assessment of the zones which use the conduit under consideration. Risk assessment should take into consideration the likelihood and consequences of security of a zone or conduit being compromised. Risk assessment may be qualitative, semi-quantitative, or quantitative. SL(target) determines the required effectiveness of countermeasures, devices, and systems that need to be in place to prevent security of the zone or conduit from being compromised.

Countermeasures can be:

a) technical countermeasures (firewalls, anti-virus software, etc.);

b) administrative countermeasures (policies and procedures);

c) physical countermeasures (locked doors, etc.).

Factors that influence the determination of SL(target) for a zone and conduit are:

d) network architecture with defined zone boundaries and conduits;

e) SL(target) of the zones with which the zone under consideration will communicate;

f) SL(target) of conduit, if assigned, used for communication by the zone;

g) physical access to devices and systems within the zone.

Within the zone, computing the target security level should be based on layers of security and their impact on the whole.

5.11.2.3 SL(achieved) – achieved security level

SL(achieved) of a zone or conduit depends on inherent security properties of devices and systems within the zone or conduit and/or properties of countermeasures that are in place to prevent the security of the zone or conduit from being compromised. SL(achieved) is a function of time and decreases with time due to degradation of countermeasures, new vulnerabilities, adjusted threats or attack methods, breach in security layers, and inherent security properties of devices and systems until they are reviewed, updated, or upgraded.

The objective is to ensure that at any given time SL(achieved) of a zone or conduit is greater than or equal to the SL(target) for the zone or conduit.

5.11.2.4 SL(capability) – security level capability of countermeasures, devices or systems

SL(capability) is defined for countermeasures and inherent security properties of devices and systems within a zone or conduit that contribute to the security of a zone or conduit. It is a measure of the effectiveness of the countermeasure, device, or system for the security property that they address.

Examples of security properties that may be addressed by a countermeasure, device or system are given below:

a) proving peer entity authenticity;

b) preserving authenticity and integrity of messages;

c) preserving confidentiality of messages/information/communication;

d) ensuring accountability (non-repudiation);

e) enforcing access control policies;

f) preventing denial-of-service attacks;

g) maintaining platform trustworthiness;

h) detecting tampering;

i) monitoring security status.

SL(capability) of a countermeasure, device or system within a zone or conduit contributes to the SL(achieved) based on the relevant security properties addressed by countermeasures, devices or systems for that zone or conduit.

5.11.3 Factors influencing SL(achieved) of a zone or conduit

5.11.3.1 General

There are several factors that contribute to the SL(achieved) of a zone or conduit. The SL(achieved) of a zone or conduit can be expressed as a function of these factors:

SL(achieved) = f(x1, … , xn, t)

Where the factors xi (1 < = i < = n) include but are not limited to the following:

x1: SL(capability) of countermeasures associated with the zone or conduit and inherent security properties of devices and systems within a zone or conduit;

x2: SL (achieved) by the zones with which communication is to be established;

x3: Type of conduits and security properties associated with the conduits used to communicate with other zones (applicable to zones only);

x4: Effectiveness of countermeasures;

x5: Audit and testing interval of countermeasures and inherent security properties of devices and systems within a zone or conduit;

x6: Attacker expertise and resources available to attacker;

x7: Degradation of countermeasures and inherent security properties of devices and systems;

x8: Intrusion detection;

t: Time.

These parameters are described in more detail in the following subclauses.

5.11.3.2 SL(capability) of countermeasures and inherent security properties

The relevant security properties addressed by countermeasures, devices and systems within the zone or conduit and their effectiveness contribute to the SL(achieved) by a zone or conduit.

Countermeasures may be capable of addressing several security properties, but if none of them is relevant to the security of the zone or conduit, such countermeasures do not contribute to SL(achieved) of that zone or conduit. Similarly, if the inherent security properties of devices and systems within the zone or conduit are not relevant to the security of the zone or conduit, they do not contribute to SL(achieved) of that zone or conduit.

5.11.3.3 SL(achieved) by zones with which communication is to be established

Security of a zone or conduit cannot be considered in isolation. It is impacted by the SL(achieved) of the zones with which it communicates.

For example, consider a SIS in a chemical plant communicating with a DCS over a serial link. Assuming that the DCS and SIS are in two separate zones, the SL(achieved) by the SIS zone will be influenced by SL(achieved) by the DCS zone.

5.11.3.4 Type of conduits and security properties associated with the conduits

The conduit may be a point-to-point link, LAN, or WAN with inherent security properties. The conduit may include countermeasures that enhance the security properties of the conduit. The security properties of a conduit that contribute to the security of the conduit will contribute to the SL(achieved) by the conduit. The security properties of a conduit, used by a zone to communicate with other zones, will contribute to the SL(achieved) by the zone.

5.11.3.5 Effectiveness of countermeasures

Technical and administrative countermeasures can be implemented to help achieve the desired SL(target) for a zone or conduit.

Various technical countermeasures that address different security properties are available for implementation with an IACS. Technical countermeasures should address security properties relevant to the zone, but if those security properties are not effective for that zone, then their contribution to SL(achieved) by the zone is very low or none at all. Examples of technical countermeasures include intrusion detection systems (IDS), firewalls, and anti-virus software.

An evaluation of the effectiveness of technical countermeasures should take the following into consideration:

a) Development process: availability of written procedures, quality management plan, etc. This will help reduce systematic errors such as software bugs or memory leaks that may impact security.

b) Testing: level of testing for each security property addressed by the countermeasures, device, or system. Test data may also be inferred from previously assessed systems.

c) Data collection: number of times a zone or conduit was compromised due to a flaw in a similar countermeasure, device, or system; rate and criticality of vulnerabilities discovered for the countermeasure, device, or system.

Administrative countermeasures should be used when technical countermeasures are not feasible. An example of an administrative measure is restricting physical access to IACS components.

5.11.3.6 Audit and testing interval of countermeasures

The effectiveness of countermeasures and inherent security properties of devices and systems should be audited and/or tested at regular intervals based on procedures that will audit and/or test at least the security properties relevant to a zone. In some cases, the discovery of new vulnerabilities may also trigger an audit or test.

5.11.3.7 Attacker expertise and resources available to attacker

The expertise of the attacker and resources, including tools and time, available to an attacker affects SL(achieved) of a zone or conduit. Industry-accepted attacker capabilities and tools should be assumed. The time available to an attacker to compromise the security of a zone will depend on the application and countermeasures implemented for the zone or conduit.

5.11.3.8 Degradation of countermeasures

Countermeasures and inherent security properties of devices and systems will effectively degrade over time, thereby decreasing the SL(achieved) of a zone or conduit. The degradation of countermeasures and inherent security properties of devices and systems occurs due to the following:

a) discovery of new vulnerabilities;

b) improved attackers' skills;

c) attacker familiarity with existing countermeasures;

d) availability of better resources to attackers.

5.11.3.9 Intrusion detection

Countermeasures and inherent security properties of devices and systems may include intrusion detection. The time available to respond to a detected intrusion impacts the SL(achieved) of a zone and conduit.

5.11.4 Impact of countermeasures and inherent security properties of devices and systems

The use of countermeasures and inherent security properties of devices and systems to achieve the SL(target) can result in degradation in communication performance. The degradation in communication performance due to countermeasures and inherent security properties of devices and systems need to be evaluated to ensure that the minimum functional requirements of the zone are still met.

For example, speed of response is an important requirement for an IACS. Countermeasures can add latency to communication, which may not be acceptable in certain applications.

5.12 Security level lifecycle

5.12.1 General

Security levels become an important part of the security lifecycle of an IACS zone once the zone boundaries and conduits have been defined. It is important to recognize that the security level lifecycle is focused on the security level of a zone or conduit over time. It should not be confused with the lifecycle phases of the actual physical assets comprising the IACS within the zone. Although there are many overlapping and complementary activities associated with the asset lifecycle and the zone security level lifecycle, they each have different trigger points to move from one phase to another. Furthermore, a change to a physical asset may trigger a set of security level activities, or a change in security vulnerabilities or, an asset may trigger a change in the physical asset.

Figure 8 depicts the security level lifecycle. A zone is assigned a SL(target) during the Assess phase of the security lifecycle. Countermeasures are implemented during the Implement phase to meet the SL(target) for the zone. SL(achieved) by a zone depends on various factors. In order to ensure that the SL(achieved) is better or equal than the SL(target) for the zone at all times, the countermeasures are audited and/or tested and upgraded, if necessary, during the Maintain phase of the security lifecycle.

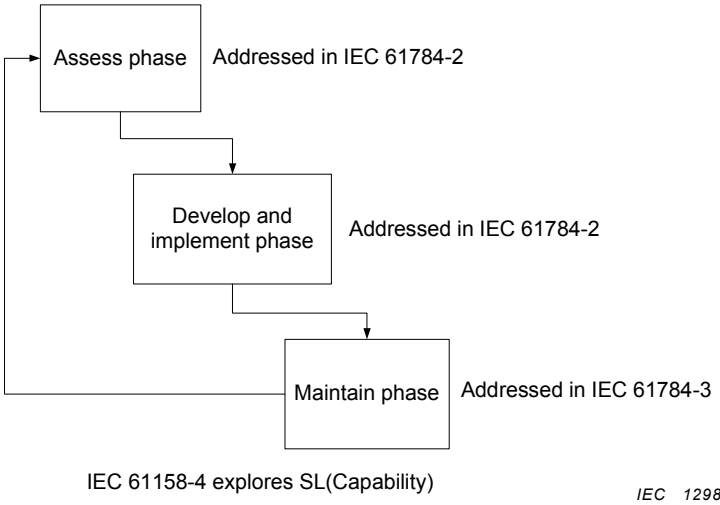

Figure 8 – Security level lifecycle

5.12.2 Assess phase

The Assess phase of the security level lifecycle includes activities shown in Figure 9. Prior to assigning SL(target) to a zone, the following need to be established:

a) zone boundaries;

b) organization's risk tolerance criteria.

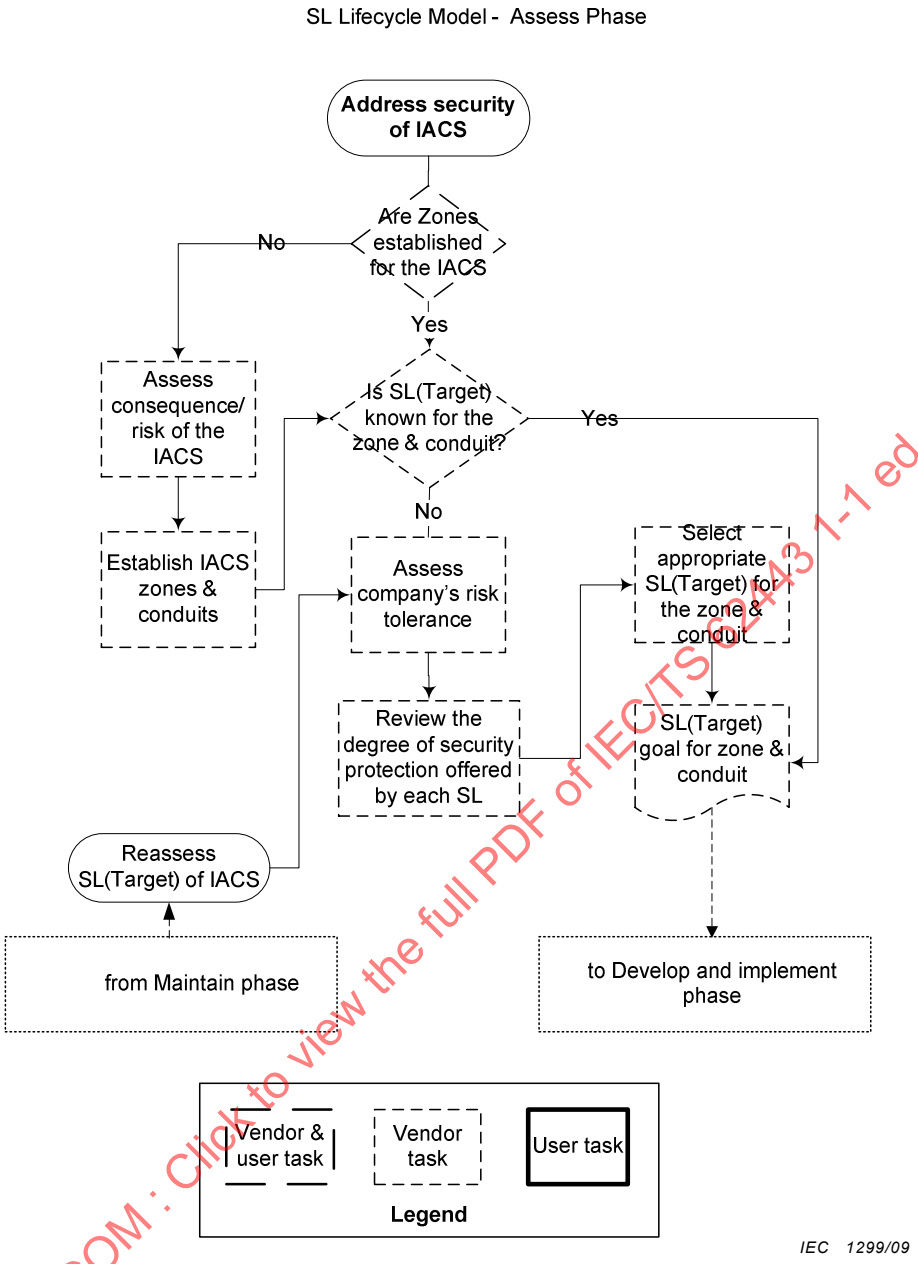

Figure 9 – Security level lifecycle – Assess phase

A risk assessment for a zone should be performed and SL(target) assigned to the zone. Details of risk assessment and other activities associated with the assess phase will be addressed in a future part of IEC 62443.

5.12.3 Develop and implement phase

Once a SL(target) has been assigned to a zone in the Assess phase, countermeasures should be implemented to reach SL(achieved) better than or equal to SL(target) for the zone. Figure 10 depicts the activities, for new and existing IACS zones, in the Implement phase of the security level lifecycle. The SL(achieved) is determined after the system has been validated against the security requirements for the zone.

Details of activities associated with the implement phase will be addressed in a future part of IEC 62443.

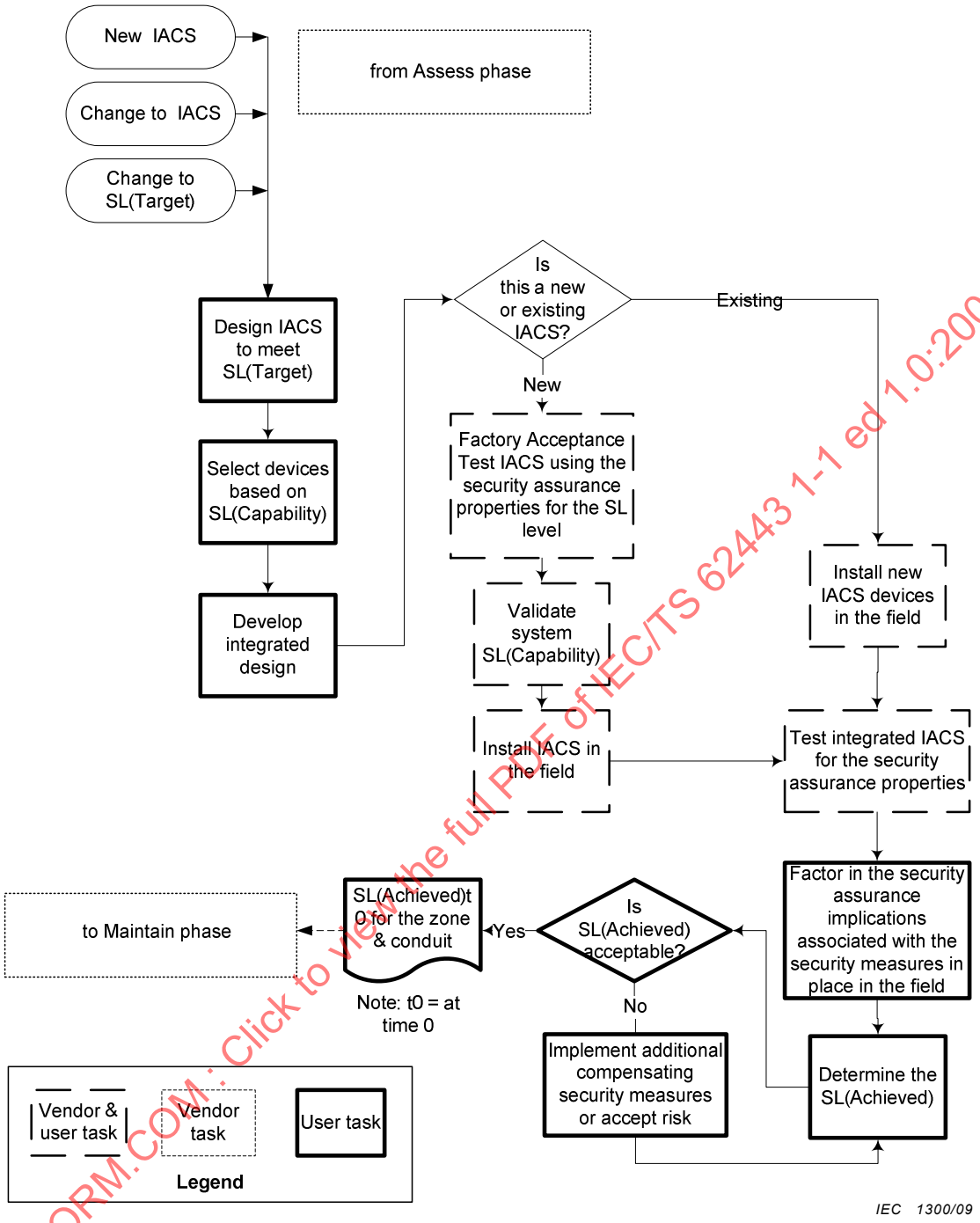

Figure 10 – Security level lifecycle – Implement phase

5.12.4 Maintain phase

Countermeasures and inherent security properties of devices and systems degrade over time. The security properties relevant to the zone, including conduits associated with the zone, should be audited and/or tested at regular intervals or whenever a new vulnerability is discovered to ensure that SL(achieved) is better than or equal to SL(target) for the zone at any time. The activities associated with maintaining the SL(achieved) by a zone are shown in Figure 11.

Details of activities associated with the maintain phase will be addressed in a future part of IEC 62443.

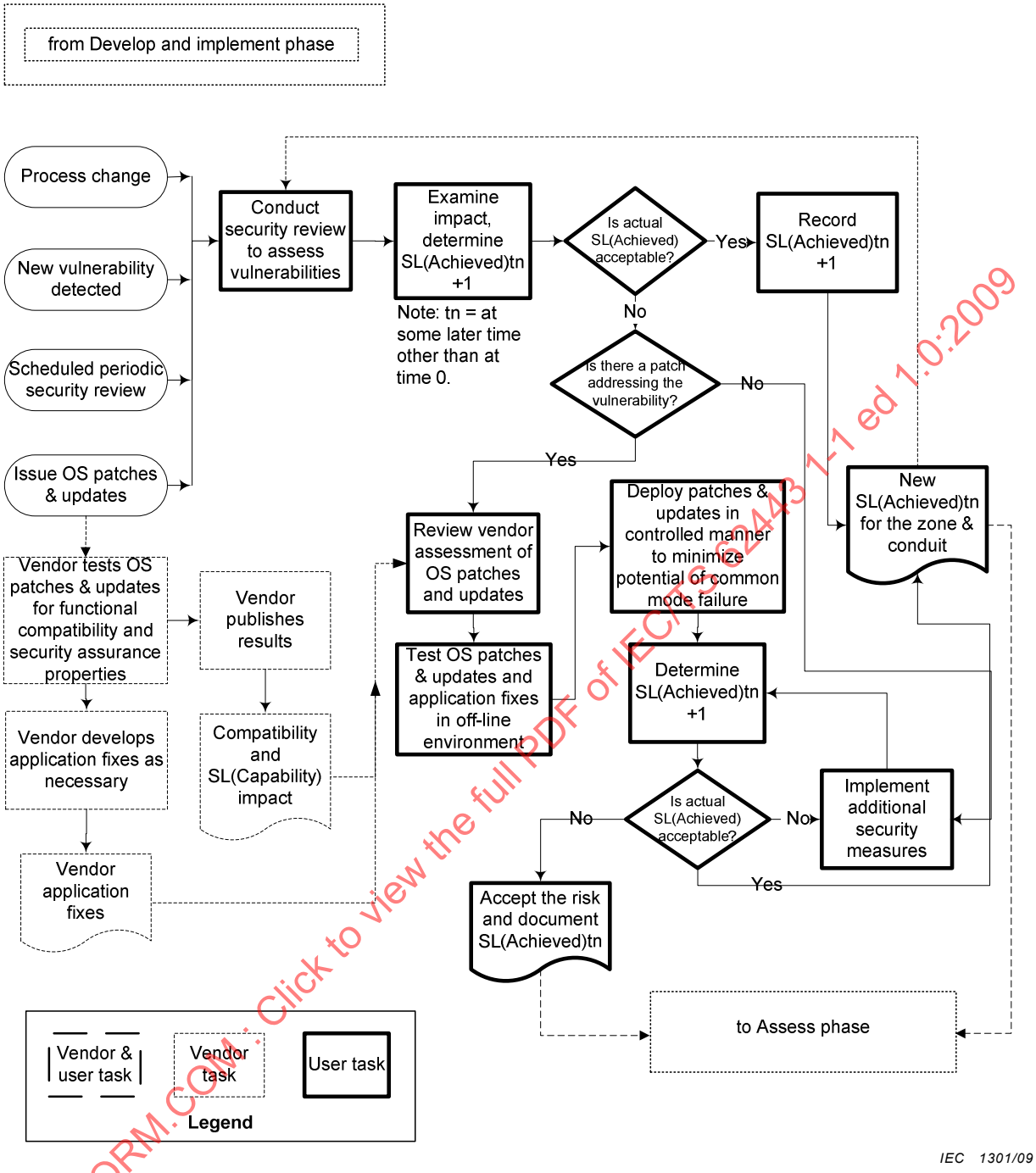

Figure 11 – Security level lifecycle – Maintain phase

6 Models

6.1 General

This clause describes a series of models that can be used in the design of an appropriate security program. The objective is to identify the security needs and important characteristics of the environment at a level of detail necessary to address security issues with a common understanding of the framework and vocabulary. These models come in various forms, including:

a) Reference models that provide the overall conceptual basis for the more detailed models that follow.

b) Asset models that describe the relationships between assets within an industrial automation and control system.

c) A reference architecture that describes the configuration of assets. A reference architecture can be unique for each enterprise or subset of the enterprise. It is unique for each situation depending on the scope of the industrial automation and control system under review.

d) A zone model that groups reference architecture elements according to defined characteristics. This provides a context for the definition of policies, procedures, and guidelines, which in turn are applied to the assets.

All of this information is used to develop a detailed program for managing the security of an industrial automation and control system.

Each of the major types of models is described in more detail in the following subclauses.

6.2 Reference models

6.2.1 Overview

A reference model establishes a frame of reference for the more detailed information that follows. The term “reference model” became popular with the success of the ISO Seven Layer model for Open Systems Interconnection (OSI). The U.S. NASA Office of Standards and Technology (NOST) defines the term as:

“*A reference model is a framework for understanding significant relationships among the entities of some environment, and for the development of consistent standards or specifications supporting that environment. A reference model is based on a small number of unifying concepts and may be used as a basis for education and explaining standards to a non-specialist.*” [8]

A reference model describes a generic view of an integrated manufacturing or production system, expressed as a series of logical levels. The reference model used by the IEC 62443 series of standards appears in Figure 12. This model is derived from the general model used in IEC 62264-1.

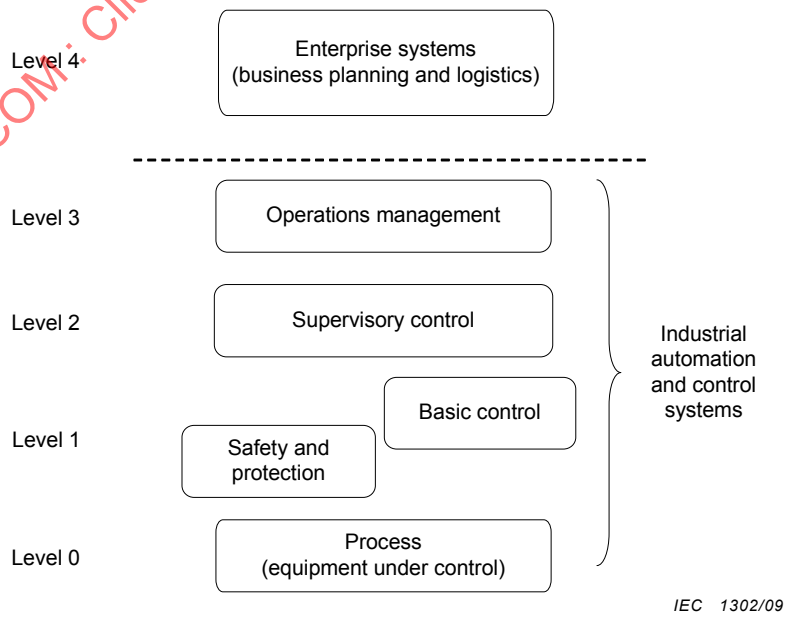

Figure 12 – Reference model for IEC 62443 standards

A slightly different view of the reference model may be used for SCADA applications. This view is shown in Figure 13.

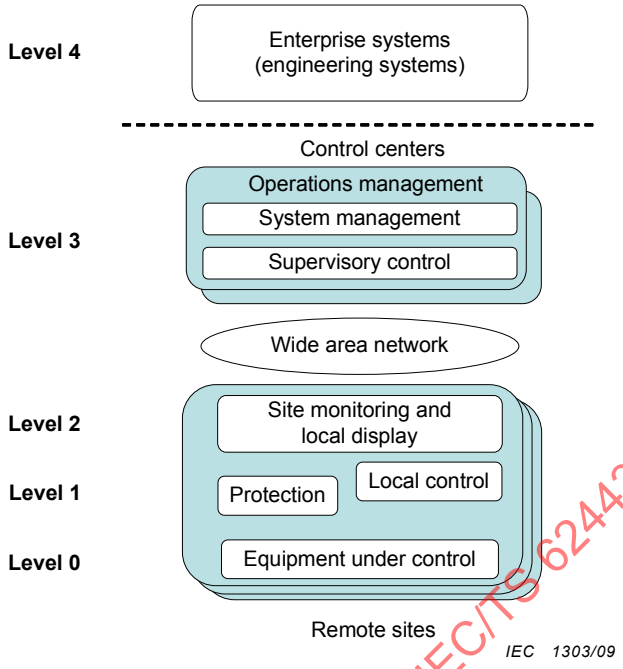

Figure 13 – SCADA reference model

6.2.2 Reference model levels

6.2.2.1 General

Both of these models consist of the same basic levels, each representing a particular class of functionality. The level definitions are based on the functional hierarchy model of IEC 62264-1 and describe the functions and activities from the process (Level 0) to the enterprise (Level 4).

The following subclauses describe each of the levels of this model in more detail.

6.2.2.2 Level 4 – Enterprise systems

This level, described as business planning and logistics in IEC 62264-1, is defined as including the functions involved in the business-related activities needed to manage a manufacturing organization. Functions include enterprise or regional financial systems and other enterprise infrastructure components such as production scheduling, operational management, and maintenance management for an individual plant or site in an enterprise. For the purposes of this technical specification, engineering systems are also considered to be in this level.

Level 4 activities include the following activities:

a) Collecting and maintaining raw material and spare parts usage and available inventory, and providing data for purchase of raw material and spare parts.

b) Collecting and maintaining overall energy use and available inventory and providing data for purchase of energy source.

c) Collecting and maintaining overall goods in process and production inventory files.

d) Collecting and maintaining quality control files as they relate to customer requirements.

e) Collecting and maintaining machinery and equipment use and life history files necessary for preventive and predictive maintenance planning.

f) Collecting and maintaining manpower use data for transmittal to personnel and accounting.

g) Establishing the basic plant production schedule.

h) Modifying the basic plant production schedule for orders received based on resource availability changes, energy sources available, power demand levels, and maintenance requirements.

i) Developing optimum preventive maintenance and equipment renovation schedules in coordination with the basic plant production schedule.

j) Determining the optimum inventory levels of raw materials, energy sources, spare parts, and goods in process at each storage point. These functions also include materials requirements planning (MRP) and spare parts procurement.

k) Modifying the basic plant production schedule as necessary whenever major production interruptions occur.

l) Capacity planning based on all of the above activities.

6.2.2.3 Level 3 – Operations management

Level 3 includes the functions involved in managing the work flows to produce the desired end products. Examples include dispatching production, detailed production scheduling, reliability assurance, and site-wide control optimization.

Level 3 activities include the following activities:

a) Reporting on area production including variable manufacturing costs.

b) Collecting and maintaining area data on production, inventory, manpower, raw materials, spare parts, and energy usage.

c) Performing data collection and off-line analysis as required by engineering functions. This may include statistical quality analysis and related control functions.

d) Carrying out needed personnel functions such as: work period statistics (for example: time, task), vacation schedule, work force schedules, union line of progression, and in-house training and personnel qualification.

e) Establishing the immediate detailed production schedule for its own area including maintenance, transportation, and other production-related needs.

f) Locally optimizing the costs for its individual production area while carrying out the production schedule established by the Level 4 functions.

g) Modifying production schedules to compensate for plant production interruptions that may occur in its area of responsibility.

6.2.2.4 Level 2 – Supervisory control

Level 2 includes the functions involved in monitoring and controlling the physical process. There are typically multiple production areas in a plant such as distillation, conversion, blending in a refinery or the turbine deck, and coal processing facilities in a utility power plant.

Level 2 functions include the following:

a) operator human-machine interface;

b) operator alarms and alerts;

c) supervisory control functions;

d) process history collection.

6.2.2.5 Level 1 – Local or basic control

Level 1 includes the functions involved in sensing and manipulating the physical process.

Process monitoring equipment reads data from sensors, executes algorithms if necessary, and maintains process history. Examples of process monitoring systems include tank gauging systems, continuous emission monitors, rotating equipment monitoring systems, and temperature indicating systems. Process control equipment is similar. It reads data from

sensors, executes a control algorithm, and sends an output to a final element (e.g., control valves or damper drives). Level 1 controllers are directly connected to the sensors and actuators of the process.

Level 1 includes continuous control, sequence control, batch control, and discrete control. Many modern controllers include all types of control in a single device.

Also included in Level 1 are safety and protection systems[4] that monitor the process and automatically return the process to a safe state if it exceeds safe limits. This category also includes systems that monitor the process and alert an operator of impending unsafe conditions.

Safety and protection systems have traditionally been implemented using physically separate controllers, but more recently it has become possible to implement them using a method known as logical separation, within a common infrastructure. The depiction shown in this reference model was chosen to emphasize the need for this separation (logical or physical) to ensure the integrity of the safety functions. Level 1 equipment includes, but is not limited to the following:

a) DCS controllers;

b) PLCs;

c) RTUs.

Safety and protection systems often have additional safety requirements that may not be consistent or relevant to cybersecurity requirements. These systems include the safety systems in use in chemical and petrochemical plants as identified in the IEC 61511 series of standards, nuclear plant safety or safety-related systems as identified in the IEC 61513 series, and protective functions as identified in IEEE Power Engineering Society standards.

6.2.2.6 Level 0 – Process

Level 0 is the actual physical process. The process includes a number of different types of production facilities in all sectors including, but not limited to, discrete parts manufacturing, hydrocarbon processing, product distribution, pharmaceuticals, pulp and paper, and electric power.

Level 0 includes the sensors and actuators directly connected to the process and process equipment.

6.3 Asset models

6.3.1 Overview

Modern control systems are complex computer networks with many interconnected components that perform a variety of tasks to safely and efficiently operate chemical plants, auto parts manufacturing plants, pipelines, electric generation facilities, transmission and distribution networks, and many other types of industrial facilities, transportation systems, and utilities.

At one time these systems were isolated from other computers in the enterprise and used proprietary hardware, software, and networking protocols. This is no longer the case as control system vendors have adapted COTS information technology because of its cost advantages, and business needs have driven the integration of control systems with business information systems.

---

4 These systems are referred to as safety instrumented systems in standards such as the IEC 61511 series.

From a security perspective, the concern is with the control equipment itself, the users of that equipment, the connections between control system components, and the interconnections with business systems and other networks.

This document is intended to apply to the broad range of industrial automation and control systems used across multiple industry segments. Therefore, the asset model should start at a high level and be generic enough to fit the many situations where control systems are deployed. See Figure 14.

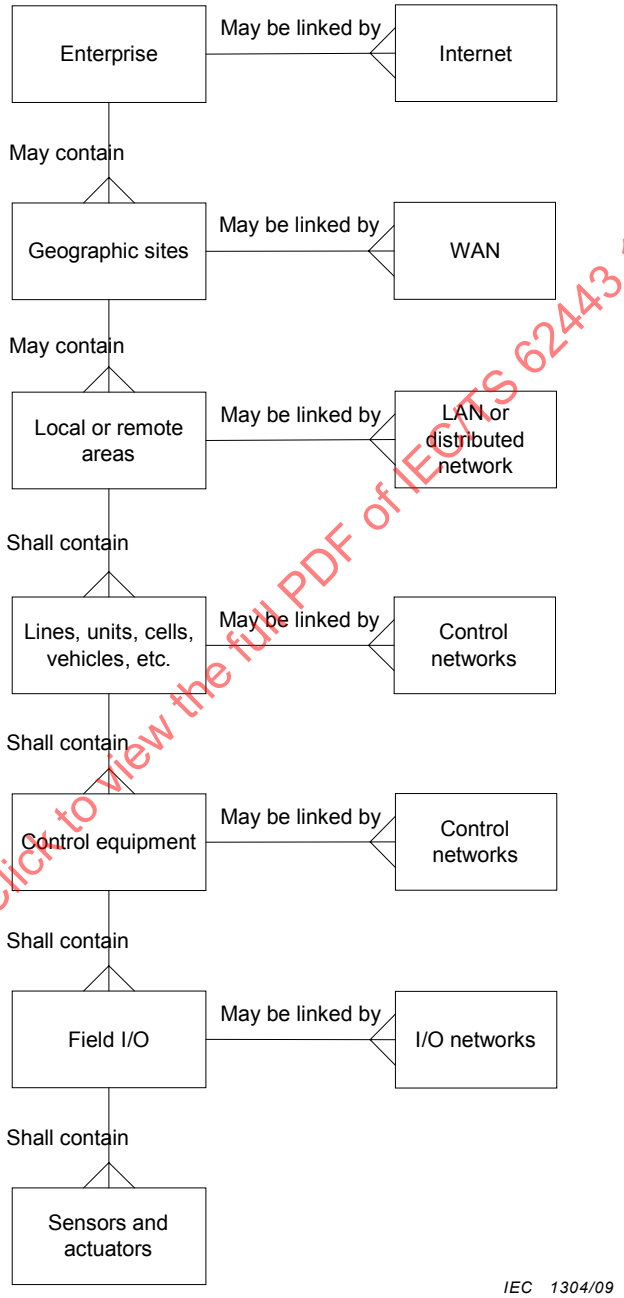

Figure 14 – Process manufacturing asset model example

Because networks play an important role in security, the asset model explicitly includes the network elements typically present at each level of the hierarchy. At each level, the equipment (or facilities) is linked together by the appropriate type of network. Although the networks themselves may be linked together, this model does not depict that linkage.