IEC TR 63069

Edition 1.0 2019-05

TECHNICAL REPORT

colour inside

Industrial-process measurement, control and automation – Framework for functional safety and security

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

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

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

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

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 It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

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

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC TR 63069

Edition 1.0 2019-05

TECHNICAL REPORT

colour inside

Industrial-process measurement, control and automation – Framework for functional safety and security

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 13.110; 25.040.40; 29.020

ISBN 978-2-8322-6925-1

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

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INDUSTRIAL-PROCESS MEASUREMENT, CONTROL AND AUTOMATION – FRAMEWORK FOR FUNCTIONAL SAFETY AND SECURITY

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a Technical Report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC TR 63069 has been prepared by IEC technical committee TC 65: Industrial-process measurement, control and automation.

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

Draft DTR	Report on voting
65/698/DTR	65/713A/RVDTR

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

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

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

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

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 document using a colour printer.

INTRODUCTION

0.1 Purpose of this document

Many sector specific guides, standards and technical specifications have been developed in the fields of safety and security. However, a generic document for framework for safety and security is largely expected by industry actors. Even the terms "safety" and "security" are sometimes used for different meanings in these documents. As a result, it can be difficult to apply them holistically at the same time to a manufacturing system.

0.2 Background

Security has become a new factor to be considered in system engineering. The parts of the IEC 61508 series published in 2010 took into account that security can impact functional safety.

In IEC TC 65 (Industrial-process measurement, control and automation), considerable concerns arose with respect to the impacts of security incidents to safety functions in IACS (industrial automation and control systems); many complex systems of that kind are becoming connected systems (particularly by interaction based on wireless connectivity from sensors/actuators to complete plants, grids, etc.) for maintenance and operations. The overall question was: "How to design and manage safety and security – in cooperation, integrated, or separate system?"

0.3 Issues on the terminology

Definitions of some terms, such as "safety", "security" and "risk", are sometimes different in different documents. Although they are consistent in a set of documents in each area of safety and security, they can be inconsistent when both standards are applied at the same time. From these reasons, the terminology is carefully used in this document.

0.4 Target audience

The target audience of this document includes, but is not limited to,

- asset owners (including those responsible for concept and governance),
- system integrators (including those responsible for design and realisation),
- product suppliers (including those responsible for design and realisation),
- service providers (including operators and maintainers), and
- authorities (including those responsible for assessment and audit).

INDUSTRIAL-PROCESS MEASUREMENT, CONTROL AND AUTOMATION – FRAMEWORK FOR FUNCTIONAL SAFETY AND SECURITY

1 Scope

This document explains and provides guidance on the common application of IEC 61508 (all parts) and IEC 62443 (all parts) in the area of industrial-process measurement, control and automation.

This document can apply to other industrial sectors where IEC 61508 (all parts) and IEC 62443 (all parts) are applied.

NOTE Usage or reference of this document for industry specific sector standards is encouraged.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 62443 (all parts), *Security for industrial automation and control systems*

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions defined for this document

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

NOTE Within this document, new terms and definitions are created only if not provided by the IEC 61508 series or the IEC 62443 series.

3.1.1
incident handling
actions of detecting, reporting, assessing, responding to, dealing with, and learning from security incidents

[SOURCE: ISO/IEC 27035-1:2016, 3.6, modified – The words "information security incidents" has been replaced by "security incidents".]

3.1.2
incident response
actions taken to mitigate or resolve a security incident, including those taken to protect and restore the normal operational conditions of an IACS and the information stored in it

[SOURCE: ISO/IEC 27035-1:2016, 3.7, modified – The words "information security incident" were replaced by "security incident", and "information system" was replaced by "IACS".]

3.1.3
safety domain
safety activities carried out by assigned persons or organizations and their outcomes according to IEC 61508 (all parts)

3.1.4
security domain
security activities carried out by assigned persons or organizations and their outcomes according to IEC 62443 (all parts)

3.1.5
security environment
area of consideration where all relevant security countermeasures are in place and effective

3.1.6
access
ability and means to communicate with or otherwise interact with a system in order to use system resources

Note 1 to entry: Access may involve physical access (authorization to be allowed physically in an area, possession of a physical key lock, PIN code, or access card or biometric attributes that allow access) or logical access (authorization to log in to a system and application, through a combination of logical and physical means).

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

3.1.7
architecture
specific configuration of hardware and software elements in a system

[SOURCE: IEC 61508-4:2010, 3.3.4]

3.1.8
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 1 to entry: 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.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.6]

3.1.9
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

Note 1 to entry: 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.

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

3.1.10
availability
ability of an item to be in a state to perform a required function under given conditions at a given instant or over a given time interval, assuming that the required external resources are provided

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

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

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

[SOURCE: IEC TS 62443-1-1:2009, 3.2.16]

3.1.11
confidentiality
assurance that information is not disclosed to unauthorized individuals, processes, or devices

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

3.1.12
countermeasure
action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken

Note 1 to entry: The term "control" is also used to describe this concept in some contexts. The term countermeasure has been chosen for IEC TS 62443-1-1 to avoid confusion with the term "control" in the context of process control.

Note 2 to entry: The words "minimizing the harm" in this definition do not relate to functional safety.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.33, modified – Addition of Note 2 to entry.]

3.1.13
dangerous failure
failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:

a) prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or

b) decreases the probability that the safety function operates correctly when required

[SOURCE: IEC 61508-4:2010, 3.6.7]

3.1.14
defence in depth
provision of multiple security protections, especially in layers, with the intent to delay if not prevent an attack

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

- attackers are faced with breaking through or bypassing each layer without being detected;
- a flaw in one layer can be mitigated by capabilities in other layers;
- a system security becomes a set of layers within the overall network security.

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

3.1.15
essential function
function or capability that is required to maintain health, safety, the environment and availability for the equipment under control

Note 1 to entry: Essential functions include, but are not limited to, the safety instrumented function (SIF), the control function and the ability of the operator to view and manipulate the equipment under control. The loss of essential functions is commonly termed loss of protection, loss of control and loss of view respectively. In some industries additional functions such as history may be considered essential.

[SOURCE: IEC 62443-3-3:2013, 3.1.22]

3.1.16
functional safety
part of the overall safety relating to the EUC and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures

[SOURCE: IEC 61508-4:2010, 3.1.12]

3.1.17
harm
physical injury or damage to the health of people or damage to property or the environment

[SOURCE: IEC 61508-4:2010, 3.1.1]

3.1.18
hazard
potential source of harm

Note 1 to entry: The term includes danger to persons arising within a short time scale (for example, fire and explosion) and also those that have a long-term effect on a person’s health (for example, release of a toxic substance).

[SOURCE: IEC 61508-4:2010, 3.1.2]

3.1.19
incident
event that is not part of the expected operation of a system or service that causes or may cause, an interruption to, or a reduction in, the quality of the service provided by the system

[SOURCE: IEC 62443-2-1:2010, 3.1.18]

3.1.20
industrial automation and control systems
IACS
collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process

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

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

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

3.1.21
integrity
quality of a system reflecting the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data

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

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

3.1.22
risk
<safety> combination of the probability of occurrence of harm and the severity of that harm

Note 1 to entry: For more discussion on this concept see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6, modified – The domain has been added between angle brackets.]

3.1.23
risk
<security> expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence

[SOURCE: IEC TS 62443-1-1:2009, 3.2.87, modified – The domain has been added between angle brackets.]

3.1.24
safe state
state of the EUC when safety is achieved

[SOURCE: IEC 61508-4:2010, 3.1.13, modified – Deletion of the note.]

3.1.25
safety
freedom from unacceptable risk

[SOURCE: IEC 61508-4:2010, 3.1.11]

3.1.26
safety function
function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event

EXAMPLE Examples of safety functions include:

- functions that are required to be carried out as positive actions to avoid hazardous situations (for example switching off a motor); and
- functions that prevent actions being taken (for example preventing a motor starting).

[SOURCE: IEC 61508-4:2010, 3.5.1]

3.1.27
safety integrity
probability of an E/E/PE safety-related system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time

Note 1 to entry: The higher the level of safety integrity, the lower the probability that the safety-related system will fail to carry out the specified safety functions or will fail to adopt a specified state when required.

Note 2 to entry: There are four levels of safety integrity (see 3.5.8 of IEC 61508-4:2010).

Note 3 to entry: In determining safety integrity, all causes of failures (both random hardware failures and systematic failures) that lead to an unsafe state should be included, for example hardware failures, software induced failures and failures due to electrical interference. Some of these types of failure, in particular random hardware failures, may be quantified using such measures as the average frequency of failure in the dangerous mode of failure or the probability of a safety-related protection system failing to operate on demand. However, safety integrity also depends on many factors that cannot be accurately quantified but can only be considered qualitatively.

Note 4 to entry: Safety integrity comprises hardware safety integrity (see 3.5.7 of IEC 61508-4:2010) and systematic safety integrity (see 3.5.6 of IEC 61508-4:2010).

Note 5 to entry: This definition focuses on the reliability of the safety-related systems to perform the safety functions.

[SOURCE: IEC 61508-4:2010, 3.5.4, modified – The text between brackets has been deleted.]

3.1.28
safety integrity level
SIL
discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

Note 1 to entry: The target failure measures (see 3.5.17 of IEC 61508-4:2010) for the four safety integrity levels are specified in Tables 2 and 3 of IEC 61508-1.

Note 2 to entry: Safety integrity levels are used for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems.

Note 3 to entry: A safety integrity level (SIL) is not a property of a system, subsystem, element or component. The correct interpretation of the phrase "SIL *n* safety-related system" (where *n* is 1, 2, 3 or 4) is that the system is potentially capable of supporting safety functions with a safety integrity level up to *n*.

[SOURCE: IEC 61508-4:2010, 3.5.8]

3.1.29
safety-related system
designated system that both

– implements the required safety functions necessary to achieve or maintain a safe state for the EUC; and

– is intended to achieve, on its own or with other E/E/PE safety-related systems and other risk reduction measures, the necessary safety integrity for the required safety functions

Note 1 to entry: The term refers to those systems, designated as safety-related systems, that are intended to achieve, together with the other risk reduction measures (see 3.4.2 of IEC 61508-4:2010), the necessary risk reduction in order to meet the required tolerable risk (see 3.1.7 of IEC 61508-4:2010). See also Annex A of IEC 61508-5:2010.

Note 2 to entry: Safety-related systems are designed to prevent the EUC from going into a dangerous state by taking appropriate action on detection of a condition which may lead to a hazardous event. The failure of a safety-related system would be included in the events leading to the determined hazard or hazards. Although there may be other systems having safety functions, it is the safety-related systems that have been designated to achieve, in their own right, the required tolerable risk. Safety-related systems can broadly be divided into safety-related control systems and safety-related protection systems.

Note 3 to entry: Safety-related systems may be an integral part of the EUC control system or may interface with the EUC by sensors and/or actuators. That is, the required safety integrity level may be achieved by implementing the safety functions in the EUC control system (and possibly by additional separate and independent systems as well) or the safety functions may be implemented by separate and independent systems dedicated to safety.

Note 4 to entry: A safety-related system may

a) be designed to prevent the hazardous event (i.e. if the safety-related systems perform their safety functions then no harmful event arises);

b) be designed to mitigate the effects of the harmful event, thereby reducing the risk by reducing the consequences;

c) be designed to achieve a combination of a) and b).

Note 5 to entry: A person can be part of a safety-related system. For example, a person could receive information from a programmable electronic device and perform a safety action based on this information, or perform a safety action through a programmable electronic device.

Note 6 to entry: A safety-related system includes all the hardware, software and supporting services (for example, power supplies) necessary to carry out the specified safety function (sensors, other input devices, final elements (actuators) and other output devices are therefore included in the safety-related system).

Note 7 to entry: A safety-related system may be based on a wide range of technologies including electrical, electronic, programmable electronic, hydraulic and pneumatic.

[SOURCE: IEC 61508-4:2010, 3.4.1]

3.1.30
security

a) measures taken to protect a system

b) condition of a system that results from the establishment and maintenance of measures to protect the system

c) condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss

d) capability of a computer-based system to provide adequate confidence that unauthorized persons and systems can neither modify the software and its data nor gain access to the system functions, and yet to ensure that this is not denied to authorized persons and systems

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

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

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

3.1.31
security incident
adverse event in a system or network, or the threat of the occurrence of such an event

[SOURCE: IEC TS 62443-1-1:2009, 3.2.106]

3.1.32
security level
SL
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

[SOURCE: IEC TS 62443-1-1:2009, 3.2.108, modified – The abbreviated term "SL" has been added.]

3.1.33
security patch
software patch that is relevant to the security of a software component

Note 1 to entry: For the purpose of this definition, firmware is considered software.

Note 2 to entry: Software patches may address known or potential vulnerabilities, or simply improve the security of the software component, including its reliable operation.

[SOURCE: IEC 62443-2-4:2015, 3.1.17]

3.1.34
security perimeter
boundary (logical or physical) of the domain in which a security policy or security architecture applies, i.e., the boundary of the space in which security services protect system resources

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

3.1.35
security zone
grouping of logical or physical assets that share common security requirements

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

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

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

3.1.36
systematic capability
measure (expressed on a scale of SC 1 to SC 4) of the confidence that the systematic safety integrity of an element meets the requirements of the specified SIL, in respect of the specified element safety function, when the element is applied in accordance with the instructions specified in the compliant item safety manual for the element

Note 1 to entry: Systematic capability is determined with reference to the requirements for the avoidance and control of systematic faults (see IEC 61508-2 and IEC 61508-3).

Note 2 to entry: What is a relevant systematic failure mechanism will depend on the nature of the element. For example, for an element comprising solely software, only software failure mechanisms will need to be considered. For an element comprising hardware and software, it will be necessary to consider both systematic hardware and software failure mechanisms.

Note 3 to entry: A Systematic capability of SC N for an element, in respect of the specified element safety function, means that the systematic safety integrity of SIL N has been met when the element is applied in accordance with the instructions specified in the compliant item safety manual for the element.

[SOURCE: IEC 61508-4:2010, 3.5.9]

3.1.37
threat
potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm

[SOURCE: IEC TS 62443-1-1:2009, 3.2.125]

3.1.38
threat agent
causative agent of a threat action

[SOURCE: IEC TS 62443-1-1:2009, 3.2.127]

3.1.39
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

[SOURCE: IEC TS 62443-1-1:2009, 3.2.135]

3.2 Abbreviated terms

BPCS	Basic Process Control System
DCS	Distributed Control System
DoS	Denial of Service
E/E/PE	Electrical/Electronic/Programmable Electronic
EUC	Equipment Under Control
HFT	Hardware Fault Tolerance
IACS	Industrial Automation and Control Systems
PLC	Programmable Logic Controller
RTU	Remote Terminal Unit
SC	Systematic Capability
SCADA	Supervisory Control And Data Acquisition
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SL	Security Level

3.3 Explanation for common terms with different definitions

Some terms have different definitions in the IEC 61508 series and IEC 62443 series. For them, explanation is given in Table 1.

The meaning of each appearance of these terms in the body of this document is clarified by indicating which definition is intended in the context as follows.

The domain identification "<safety>" following a term indicates that the meaning of this term is intended as defined by IEC 61508 (all parts). Similarly, the domain identification "<security>" indicates the meaning is intended as defined by IEC 62443 (all parts).

NOTE 1 When a term that can have a domain identifier is used without domain identifier, the term is intended as a general term.

Table 1 provides additional information on the existing terms and definitions of IEC 61508 (all parts) and IEC 62443 (all parts).

NOTE 2 Table 1 does not include notes to entry for the definitions.

Table 1 – Terms with multiple definitions

Term	Definition from the IEC 61508 series	Definition from the IEC 62443 series	Remark
safety	freedom from unacceptable risk [SOURCE: IEC 61508-4:2010, 3.1.11]	freedom from unacceptable risk [SOURCE: IEC TS 62443-1-1:2009, 3.2.94]	Both definitions refer to risk <safety>. NOTE Safety is related to the aspects of functional safety in the IEC 61508 series only and might be understood differently within other standards (e.g. electrical safety or mechanical safety).

Term	Definition from the IEC 61508 series	Definition from the IEC 62443 series	Remark
security	<Not defined>	a) measures taken to protect a system b) condition of a system that results from the establishment and maintenance of measures to protect the system c) condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss d) capability of a computer-based system to provide adequate confidence that unauthorized persons and systems can neither modify the software and its data nor gain access to the system functions, and yet to ensure that this is not denied to authorized persons and systems e) prevention of illegal or unwanted penetration of, or interference with the proper and intended operation of an industrial automation and control system [SOURCE: IEC TS 62443-1-1:2009, 3.2.99]	The IEC Guide 120 provides a compact and useful definition: condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences [SOURCE: IEC Guide 120: 2008, 3.13]
risk	combination of the probability of occurrence of harm and the severity of that harm [SOURCE: IEC 61508-4:2010 , 3.1.6]	expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence [SOURCE: IEC TS 62443-1-1:2009 , 3.2.87]	The difference in the definition results from the different views of security vs. safety in respect to the consequence. Where the consequence in safety is related to harm, the consequence related to security incidents might not be known. – Risk (safety): • hazard causes; • more focused on harm. – Risk (security): • threat/attack causes; • more focus on business, financial and operational impacts.
safety function	function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event (see 3.4.1 and 3.4.2) [SOURCE: IEC 61508-4:2010, 3.5.1]	<Not defined>	The term is only needed within the safety domain.

Term	Definition from the IEC 61508 series	Definition from the IEC 62443 series	Remark
safety-related system	designated system that both – implements the required safety functions necessary to achieve or maintain a safe state for the EUC; and – is intended to achieve, on its own or with other E/E/PE safety-related systems and other risk reduction measures, the necessary safety integrity for the required safety functions [SOURCE: IEC 61508-4:2010, 3.4.1]		See safety instrumented system (SIS) for IEC 62443 (all parts).
essential function	<Not defined>	function or capability that is required to maintain health, safety, the environment and availability for the equipment under control [SOURCE: IEC 62443-3-3:2013, 3.1.22]	Refer to 4.2 for further explanation.
basic process control system (BPCS)	<Not defined>	system that responds to input signals from the process, its associated equipment, other programmable systems and/or an operator and generates output signals causing the process and its associated equipment to operate in the desired manner but does not perform any safety instrumented functions (SIF) [SOURCE: IEC 62443-2-4:2015, 3.1.4]	Refer to 4.2 for further explanation.
safety instrumented system (SIS)	<Not defined>	system used to implement functional safety [SOURCE: IEC 62443-2-4:2015, 3.1.14] system used to implement one or more safety-related functions [SOURCE: IEC 62443-3-3:2013, 3.1.37]	Refer to 4.2 for further explanation.

Term	Definition from the IEC 61508 series	Definition from the IEC 62443 series	Remark
vulnerability	<Not defined>	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 [SOURCE: IEC TS 62443-1-1:2009, 3.2.135] flaw or weakness in the design, implementation, or operation and management of a component that can be exploited to cause a security compromise Note 1 to entry: Security policies typically include policies to protect confidentiality, integrity, and availability of system assets. [SOURCE: IEC 62443-2-4:2015, 3.1.23]	Vulnerability should not be compared to an error, fault or failure, as the mode of action is different. Refer to Clause 5 for further information.

Term	Definition from the IEC 61508 series	Definition from the IEC 62443 series	Remark
industrial automation and control systems (IACS)	<Not defined>	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. [IEC TS 62443-1-1:2009, 3.2.57]	Not defined within the IEC 61508 series which has a generic view of all safety-related functions realized using E/E/PE systems.
incident	<Not defined>	event that is not part of the expected operation of a system or service that causes or may cause, an interruption to, or a reduction in, the quality of the service provided by the system [IEC 62443-2-1:2010, 3.1.18]	
harm	physical injury or damage to the health of people or damage to property or the environment [IEC 61508-4:2010, 3.1.1]	<Not defined>	The definition of harm fits within the security domain as well and could be defined identically.

4 Context of security related to functional safety

4.1 Description of functions

In IEC 61508 (all parts), the main view relates to the implemented safety functions, and architectural descriptions are more related to aspects like hardware fault tolerance (HFT) and systematic capabilities. However, there is no predefined architecture common to all systems intended. Instead, performance indicators of safety integrity, such as SIL and SC are defined by IEC 61508 (all parts), allowing determining the safety performance of a dedicated IACS and the related capabilities in terms of a sufficiently low rate of random failures and an adequate set of measures for mastering systematic failures. Some parts of the IEC 62443 series use the structure of the basic process control system and the safety instrumented system within an IACS and describe a type of their installation for the process industry. However, the resulting architecture description and wording anticipates a certain implementation, which is not deemed necessary to meet the needs for safety or security. Figure 1 shows an overview of the IACS functions including safety functions, essential functions, basic control functions and complementary functions of IACS.

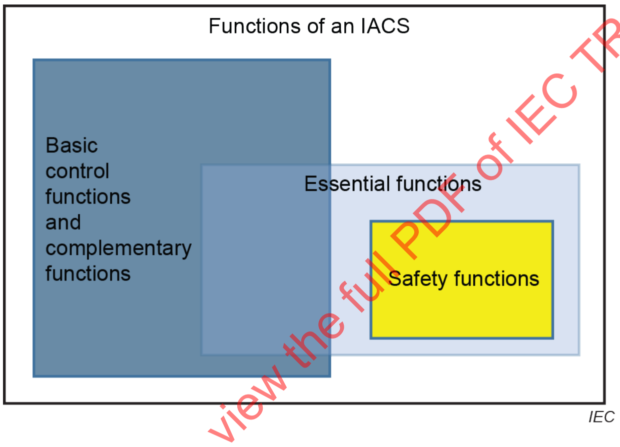

Figure 1 – Overview of functions of an IACS

Essential functions include also the safety functions of an IACS. Essential functions, which are determined by the threat-risk assessment <security>, can be implemented on a dedicated safety-related system, and also on a system which is not a safety-related system.

4.2 Security environment

This document introduces the idea of a security environment to understand an area of cooperation, as depicted in Figure 2, between the safety domain and the security domain.

The security environment as shown in Figure 3 is the overall collection of countermeasures required to ensure an efficiently protected environment for operations of the safety functions; it is however not limited to protect the safety functions only.

The security environment includes, but is not limited to, the following countermeasures:

- all countermeasures protecting the perimeters of the security environment under evaluation;
- all countermeasures concerning the interaction between different functional units at the security environment;
- all countermeasures to be applied at the functional units within the security environment.

NOTE 1 In practical applications, countermeasures might not be exclusive to the safety functions.

NOTE 2 The security environment is not the same as a "zone" as described in the IEC 62443 series.

NOTE 3 The security environment can incorporate the "defence in depth" strategy (see IEC TS 62443-1-1:2009, 5.4) for achieving sufficient resilience of an application.

Countermeasures of the security environment might be integrated into any functional unit of the technical system, including a functional unit of a safety-related system.

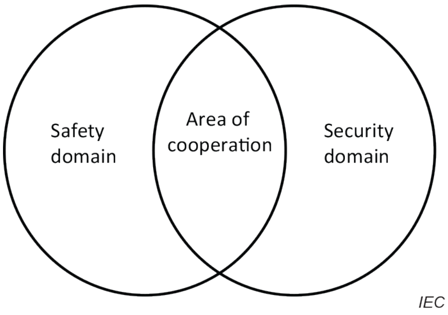

Figure 2 – Safety domain and security domain

The structures described in IEC 62443 (all parts) include a zone concept anticipating the need for clearly defined security perimeters for the individual zone and the need of having dedicated connections between zones, referred to as conduits. One or more zones or conduits may be defined as countermeasures for the security environment.

To prevent threats from exploiting vulnerabilities by attacks or human errors affecting safety functions, a security environment should be provided and maintained.

Figure 3 shows the relationships across the security environment, the operational environment and the safety-related system.

Vulnerabilities should not be understood as errors or faults of the technical system regarding the safety domain, as a vulnerability to the technical system might be introduced by an attacker and could result in failures.

EXAMPLE An attacker can use methods of social engineering by exploiting vulnerabilities of processes or people.

NOTE 4 Vulnerability management with involvement of a supplier can be a countermeasure defined by threat-risk assessment <security>.

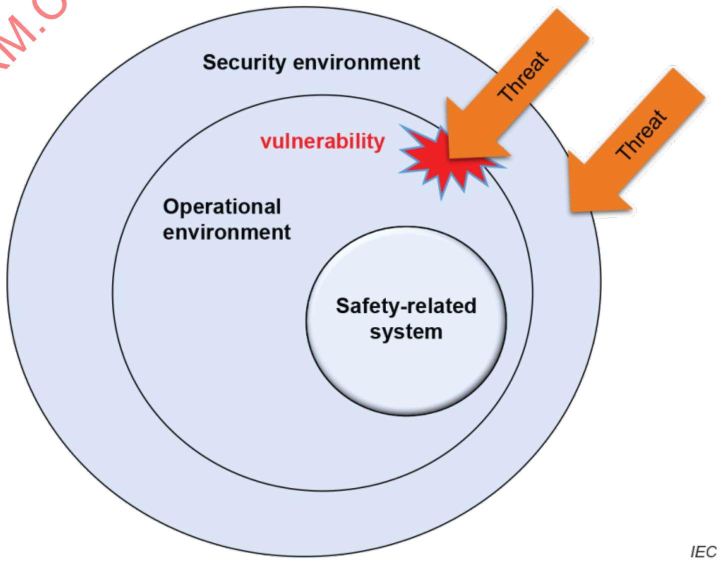

Figure 3 – Security environment

5 Guiding principles

Clause 5 specifies high level recommendations, which are called guiding principles in this document, for security considerations with relation to safety functions of IACS.

1) Guiding principle 1: protection of safety implementations

Security countermeasures should effectively prevent or guard against adverse impacts of threats to safety-related systems and their implemented safety functions. Evaluations of safety functions should be based on the assumption of effective (security) countermeasures.

EXAMPLE 1

1) Security countermeasures are expected to prevent unauthorized modification of safety relevant software, e.g. via remote access.
2) Security related investigation of safety software/code or other processes related activities prevent against unintended implementation of malware in safety critical code.

2) Guiding principle 2: protection of security implementations

The safety measures should not have an adverse impact on the effectiveness of security implementations.

NOTE Human factors are taken into account from the perspective of both the safety domain and security domain.

EXAMPLE 2

1) Safety installations are not allowed to add features, e.g. remote access to systems, not being assessed by security.
2) Safety functions might be more sensitive to DoS (denial of service) attacks and therefore being a potential target to adversely affect the availability of a system.

3) Guiding principle 3: compatibility of implementations

Security implementations and safety implementations should not have adverse contradictions.

EXAMPLE 3

1) The communication speed of a system is affected by security countermeasures and therefore adversely affecting the timing aspects of the safety function.
2) Cryptographic methods used for security are not allowed to adversely affect the communication channel protection measures used by safety.

Looking at risk mitigation for functional safety and security, there is no pre-defined priority.

6 Life cycle recommendations for co-engineering

6.1 General

Communication and interaction between the safety and security domains should be implemented throughout the life cycle to ensure a suitable security environment for the essential functions, including safety functions.

In summary, this clause recommends the following actions:

1) the development in the security and safety domains should be done in parallel and, if necessary, information should be shared between the key stakeholders;
2) resolution of conflicts should be based on consensus formed by the stakeholders in both domains;
3) before installation and commissioning for operation, the stakeholders from both domains should ensure that the security countermeasures are compatible with the operation and maintenance of the safety-related system implementation.

Functional safety is concerned with the correct functioning of safety-related systems. For systems, where safety depends on safety-related systems, security countermeasures contribute to the performance of safety functions. A set of security countermeasures should create a security environment to achieve this goal. Interaction between experts of the safety domain and of the security domain is recommended. The specific implementation of the interaction depends on the type of application and/or policy of the organization. An overview of potential interactions is shown in Figure 4.

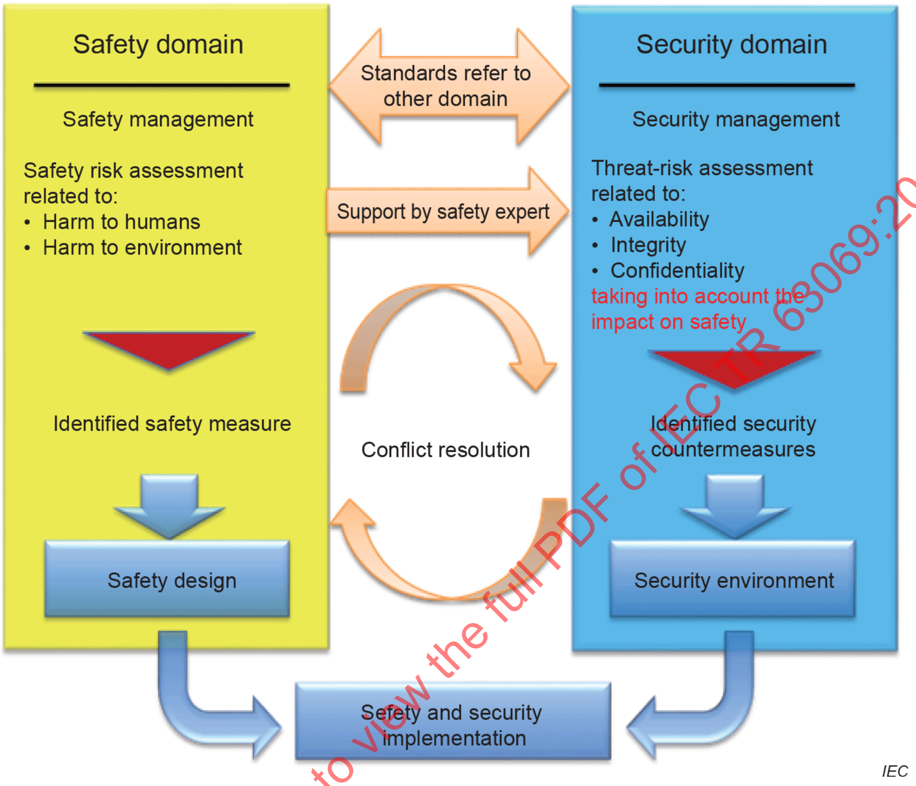
Safety domain
Safety management
Safety risk assessment related to:
• Harm to humans
• Harm to environment
Identified safety measure
Safety design
Standards refer to other domain
Support by safety expert
Conflict resolution
Security domain
Security management
Threat-risk assessment related to:
• Availability
• Integrity
• Confidentiality
taking into account the impact on safety
Identified security countermeasures
Security environment
Safety and security implementation
IEC

Figure 4 – Safety and security interaction

The safety domain should be managed by safety management according to IEC 61508 (all parts). The security domain should be managed by security management according to IEC 62443 (all parts).

Risk assessment <safety> and threat-risk assessment <security> should be done based on the result of a risk assessment at higher level.

Although risk assessment is a similar activity in the security and safety domain, it differs, because at functional safety probabilistic and non-probabilistic causes for malfunctions are evaluated in accordance with static faults. For the security domain, non-probabilistic causes in accordance with dynamic vulnerability scenarios are evaluated. Based on that, different review processes and intervals might be established. Therefore, it is advisable to have different review processes for safety and security. There is no correlation between safety integrity level (SIL) and security level (SL); these should be thought of as being independent concepts.

Security elements are not part of the risk assessment <safety>. They are covered in the threat-risk assessment <security>. However, collaboration between experts from both domains is necessary for the threat-risk assessment <security>.

During a threat-risk assessment <security>, security experts and safety experts investigate potential effects on the safety functions. The safety experts should provide descriptions of safety details on the implemented safety functions including the list of assets involved as safety-related system and their relevant data (e.g. specifications and configuration). The security expert should be able to understand the safety use cases in order to identify risks <security> with potential impact on safety.

In case of identified conflicts, the conflict resolution process should be conducted before implementation. Depending on the organization, the conflict resolution may be under different responsibilities and should be supported by all experts.

The guiding principles specified in Clause 5 should be applied throughout the life cycle. Table 2 lists recommended activities to be performed during each life cycle stage of IACS to support these guiding principles.

As there are practically many working implementations possible following the relevant requirements of IEC 61508 (all parts) or IEC 62443 (all parts), Table 2 does only represent a high-level approach towards the life cycle stages.

Table 2 – Recommended activities in life cycle stages

Life cycle stage	Guidance on activities	Guidance on documentation
Concept	Identify security threat environment. Conduct a threat-risk assessment <security> by consideration of planned safety functions as outlined in the description of safety details. Find solutions for potential conflicts between safety functions and security countermeasures. Support of a safety expert is recommended.	Document the considerations made for essential functions (including safety functions) during the security threat-risk assessment <security>. Create a security concept. Human factors should be taken into account.
Development/ Implementation	Provide relevant information on security measures (e.g. timing constraints) to ensure performance of the safety functions. Address potential conflicts of implementation of safety functions and security countermeasures. Ensure communication with security experts during development, when modifications of design are made in safety (possibly affecting the results of the security threat-risk assessment <security>). Ensure that safety-related systems are implemented entirely within the protected security environment. Make sure that used tools are covered by security countermeasures of the security environment.	Document the considerations made, especially security countermeasures, which are relevant for the security environment. Establish guidance on security for accompanying documentation. Consult with security experts to determine how access to safety is handled with security
Modification/ maintenance	Ensure communication with security experts when modifications are made in safety-related system (possibly affecting the results of the threat-risk assessment <security>). Security patches should not be applied to safety-related system without safety impact analysis and necessary verification.	Establish guidance/process on handling of modifications. Document the modifications to the considerations made, especially security countermeasures, which are relevant for the security environment.
Production	The product should be setup according to the security countermeasures defined. It should be verified that there is no known vulnerability built in the original product (e.g. malware, virus). Implemented security countermeasure should be active or set to a defined initial state.	Provide security documentation with the product.
Utilization	React to security incidents and hazardous events. Address potential conflicts of updated security countermeasures. Ensure that it is not adversely affecting the other domain.	Document latest knowledge of vulnerabilities for other projects and products.

Life cycle stage	Guidance on activities	Guidance on documentation
Support	Provide necessary information and/or patches/updates to operators.	Document configuration management changes for security patching and software updates. Report new security incidents back to product management.
Retirement (decommission)	Ensure dependence on retired security countermeasures does not expose remaining safety functions.	Document decommissioning concept.

6.2 Managing security related safety aspects

When interacting between the safety domain and the security domain, as shown in Figure 4, the following is recommended.

a) Security related safety aspects should be managed by the security domain and investigated in the threat-risk assessment <security>.

NOTE Managed by the security domain does not imply handled by security experts only.

b) Potential security impacts with impact on safety functions should be addressed by the countermeasures defined for the security environment.

c) Measures for the safety design and countermeasures for the security environment should follow the guiding principles, so that the required risk reductions are achieved in both areas.

7 Risk assessment considerations

7.1 Risk assessment at higher level

Risk assessment at higher level can be understood as a system activity covering both aspects of security and safety for identifying risks and classifying them.

The initial phase is to perform a risk assessment at higher level in order to determine the overall risk to be covered.

Risk assessment <safety> and threat-risk assessment <security> are similar processes, since both intend to take into account the consequences of threats and/or failures. However, they differ in various aspects. For example, the likelihood of vulnerability exploitation by plausible threats is nondeterministic and only qualitatively based on current experience. Security aspects cannot be quantified.

The threat-risk assessment <security> should comply with IEC 62443-2-4, IEC 62443-4-1 and IEC 62443-3-3.

The correlation between functional safety and IACS security is similar to the correlation between functional safety and electromagnetic compatibility, where a potential impact needs evaluation, but no generic settlement can be defined.

The information from a risk assessment at higher level should be available to the safety and security domains in parallel. In both domains, based on this information, the relevant risk assessments are done. Experts from both domains cooperate to address potential conflicts and compatibility issues. Identified conflicts should be resolved and can impact the safety design as well as the security design. See Figure 5.