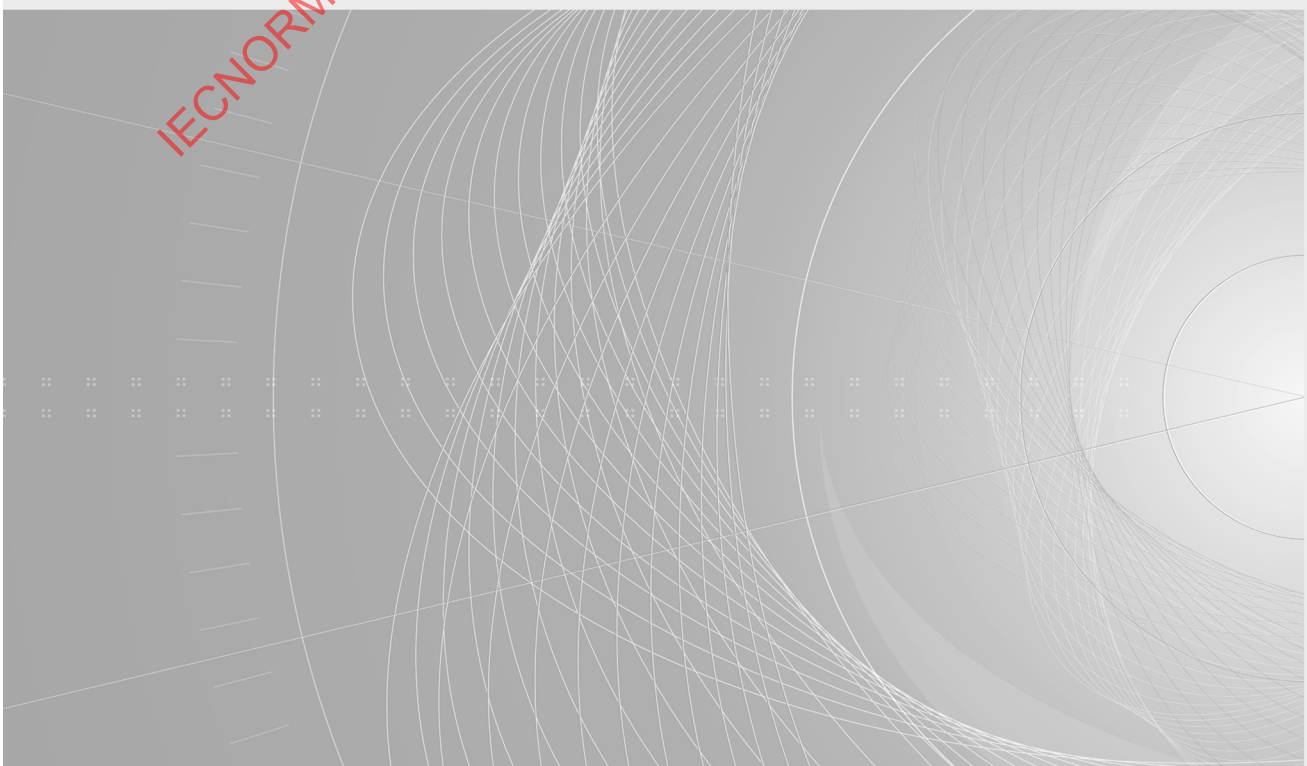
IEC TR 63074

Edition 1.0 2019-05

TECHNICAL REPORT

colour inside

Safety of machinery – Security aspects related to functional safety of safety-related control systems



IEC TR 63074:2019-05(en)

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 It also gives information on projects, replaced and withdrawn publications.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 63074

Edition 1.0 2019-05

TECHNICAL REPORT

colour inside

Safety of machinery – Security aspects related to functional safety of safety-related control systems

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 13.110; 29.020

ISBN 978-2-8322-6818-6

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

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

SAFETY OF MACHINERY – SECURITY ASPECTS RELATED TO FUNCTIONAL SAFETY OF SAFETY-RELATED CONTROL SYSTEMS

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".

Technical Report IEC TR 63074 has been prepared by IEC technical committee 44: Safety of machinery – Electrotechnical aspects.

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

DTR	Report on voting
44/842/DTR	44/843/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 publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this publication will remain unchanged until the stability 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

- 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

Industrial automation systems can be exposed to security attacks due to the fact that:

– access to the control system is possible, e.g. re-programming of machine functions (including safety);

– "convergence" between standard IT and industrial systems is increasing;

– operating systems have become present in embedded systems, e.g. IP-based protocols are replacing proprietary network protocols and data is exchanged directly from the SCADA network into the office world;

– software is developed by reusing existing third party software components;

– remote access from suppliers has become the standard way of operations / maintenance, with an increased cyber security risk regarding e.g. unauthorized access, availability and integrity.

As part of an industrial automation system, safety-related control systems of machines can also be subject to security attacks that can result in a loss of the ability to maintain safe operation of a machine.

NOTE 1 The risk potential of attack opportunities is significant seeing the trends and developments of threats and the amount of known vulnerabilities. Security objectives are mainly described in terms of confidentiality, integrity and availability, which in general need to be identified and prioritized by using a risk based approach.

Functional safety objectives consider the risk by estimating the severity of harm and the probability of occurrence of that harm: The effects of any risk (hazardous event) determine the requirements for safety integrity, (Safety Integrity Level (SIL) according to IEC 62061 or IEC 61508 or Performance Level (PL) according to ISO 13849-1).

With respect to the safety function, the security threats (internal or external) might influence the safety integrity and the overall system availability.

NOTE 2 In order to ensure the security objectives, IEC 62443-3-3 defines and recommends security requirements ("foundational requirements") to be fulfilled by the relevant system.

NOTE 3 The overall security strategy is not covered in this standard, further information is provided e.g. in IEC 62443 (all parts) or ISO/IEC 27001.

Misuse by physical manipulation is covered in some machinery functional safety standards (e.g. IEC 61496 (all parts) and ISO 14119).

NOTE 4 "Misuse by physical manipulation" is not considered to be the same as physical security in the IEC 62443 (all parts), for example in IEC 62443-2-1:2010, 4.3.3.3. Physical security means for example control (restriction) of access by means of physical obstruction.

SAFETY OF MACHINERY – SECURITY ASPECTS RELATED TO FUNCTIONAL SAFETY OF SAFETY-RELATED CONTROL SYSTEMS

1 Scope

This Technical Report gives guidance on the use of IEC 62443 (all parts) related to those aspects of security threats and vulnerabilities that could influence functional safety implemented and realized by safety-related control systems (SCS) and could lead to the loss of the ability to maintain safe operation of a machine.

NOTE 1 For example, an attack on a machine (safety function) such that it affects the availability of the machine and can result in a safety function being bypassed.

Considered security aspects of the machine with potential relation to SCS are:

– vulnerabilities of the SCS either directly or indirectly through the other parts of the machine which can be exploited by security threats that can result in security attacks (security breach);

– influence on the safety characteristics and ability of the SCS to properly perform its function(s);

– typical use case definition and application of a corresponding threat model.

NOTE 2 For other aspects of security threats and vulnerabilities, the provisions of the IEC 62443 (all parts) can apply.

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 62061, *Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems*

ISO 12100:2010, *Safety of machinery – General principles for design — Risk assessment and risk reduction*

ISO 13849-1:2015, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

3 Terms and definitions

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

3.1.1
asset
physical or logical object having either a perceived or actual value to a control system

[SOURCE: IEC 62443-3-3:2013, 3.1.1 modified –"the IACS" replaced by "a control system", removal of Note 1 to entry]

3.1.2
attack
assault on a system that derives from an intelligent threat

[SOURCE: IEC 62443-3-3:2013, 3.1.3, modified – removal of Notes 1 and 2 to entry]

3.1.3
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". In German the term "Verfügbarkeit" is also used in the sense of "instantaneous availability".

[SOURCE: IEC TS 62443-1-1:2009, 3.2.16, modified – addition of information about German terminology in Note 3]

3.1.4
confidentiality
assurance that information is not disclosed to unauthorized individuals, processes, or devices

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

3.1.5
control system
system which responds to an input from, for example, the process, other machine elements, an operator, external control equipment, and generates an output(s) causing the machine to behave in the intended manner

3.1.6
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 machine 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, modified – "EUC" replaced by "machine"]

3.1.7
functional safety
part of the safety of the machine and the machine control system which depends on the correct functioning of the safety-related control system, other technology safety-related systems and external risk reduction facilities

[SOURCE: IEC 61508-4:2010, 3.1.12, modified – "EUC" replaced by "machine", "E/E/PE" deleted]

3.1.8
machinery
machine
assembly, fitted with or intended to be fitted with a drive system consisting of linked parts or components, at least one of which moves, and which are joined together for a specific application

Note 1 to entry: The term "machinery" also covers an assembly of machines which, in order to achieve the same end, are arranged and controlled so that they function as an integral whole.

[SOURCE: ISO 12100-1:2010, 3.1, modified – removal of Note 2]

3.1.9
protective measure
measure intended to achieve risk reduction, implemented

– by the designer (inherently safe design, safeguarding and complementary protective measures, information for use) and/or
– by the user (organization: safe working procedures, supervision, permit-to-work systems; provision and use of additional safeguards; use of personal protective equipment; training)

[SOURCE: ISO 12100:2010, 3.19, modified – removal of Note]

3.1.10
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO 12100:2010, 3.12]

3.1.11
safety
freedom from risk which is not tolerable

[SOURCE: ISO/IEC Guide 51:2014, 3.14]

3.1.12
safety function
function of a machine whose failure can result in an immediate increase of the risk(s)

[SOURCE: ISO 12100, 3.30]

3.1.13
safety integrity
probability of a safety-related control system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time

[SOURCE: IEC 61508-4:2010, 3.5.4, modified –"an E/E/PE safety-related system" replaced by "a safety-related control system", removal of Notes]

3.1.14
SCS
Safety-related Control System
part of the control system of a machine which implements a safety function

Note 1 to entry: This is equivalent to SRECS of IEC 62061:2015 or one or several SRP/CS of ISO 13849-1.

[SOURCE: MT 62061, 3.2.3, modified – Note 1 removed]

3.1.15
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]

3.1.16
countermeasure
security 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

[SOURCE: IEC TS 62443-1-1:2009, 3.2.33, modified – addition of second preferred term "security countermeasure", removal of Note]

3.1.17
Security Level
SL
measure of confidence that the IACS (industrial automation control system) is free from vulnerabilities and functions in the intended manner

[SOURCE: IEC 62443-3-3:2013, 3.1.38, modified – addition of second preferred term "SL", removal of Note]

3.1.18
security risk
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 – "risk" replaced by "security risk"]

3.1.19
security 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 the exposure

[SOURCE: IEC TS 62443-1-1:2009, 3.2.88, modified –"risk assessment" replaced by "security risk assessment", "total exposure" replaced by "the exposure", removal of Notes]

3.1.20
subsystem
entity of the top-level architectural design of a safety-related system where a dangerous failure of the subsystem results in dangerous failure of a safety function

[SOURCE: IEC 61508-4:2010, 3.4.4, modified – removal of references to 3.6.7 a) within the definition]

3.1.21
threat
circumstance or event with the potential to adversely affect operations (including mission, functions, image or reputation), assets, control systems or individuals via unauthorized access, destruction, disclosure, modification of data and/or denial of service

[SOURCE: IEC 62443-3-3:2013, 3.1.44]

3.1.22
user of the machine
entity with the overall responsibility for the machine

3.1.23
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

Note 1 to entry: Vulnerabilities can be the result of intentional design choices or may be unintentional, resulting from the failure to understand the operational environment. They can 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.

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

[SOURCE: IEC/TS 62443-1-1:2009, 3.2.135, modified – addition of Note]

3.1.24
vulnerability assessment
formal description and evaluation of the vulnerabilities in a system

[SOURCE: IEC 62443-2-1:2010, 3.1.44]

4 Safety and security overview

4.1 General

The relationship between safety and security aspects can be characterized as follows:

– a machine has appropriate protective measures;
– security countermeasures applied for a machine are to be appropriate in order to avoid degradation of the performance of protective measures that implement safety function(s).

NOTE Persons who are qualified to implement security countermeasures are not necessarily the same people who are qualified to implement SCS. Therefore it is reasonable to mutually exchange information and support.

4.2 Safety objectives

Safety of machinery is based on (safety) risk assessment according to ISO 12100, or by following a type-C standard for specific machine types, in combination with the derived risk reduction measures which can be performed by safety function(s).

NOTE The risk assessment including the implemented risk reduction measures is applied by the designers during the development of machinery to enable the design of machines that are safe for their intended use.

Safety function(s) that are performed by a SCS shall achieve a safety integrity level equivalent to SIL according to IEC 62061 or PL according to ISO 13849-1.

4.3 Security objectives

In general terms security is focused mainly on achieving three objectives: confidentiality, integrity and availability.

NOTE 1 Security objectives are for example:

- Integrity against manipulations;
- Confidentiality by means of methods commonly accepted by both the security and industrial automation communities;
- Availability (usually and very generally) of machine(s) (including safety functions).

Security risks will be evaluated by using a security risk assessment in order to identify the security objectives.

A security risk assessment is based on a product / system in its environment on which threats and known vulnerabilities are applied. The aim of this activity is to derive relevant security countermeasures applied for a machine to fulfil the overall security objectives.

NOTE 2 See also 5.5 of IEC TS 62443-1-1:2009.

In the context of safety of machinery, the security countermeasures are intended to protect the ability to maintain safe operation of a machine and their implementation should not adversely affect any safety function (see Figure 1).

NOTE 3 Essential functions according to IEC 62443-3-3 include safety functions.

Due to the nature of threats and known vulnerabilities, the security risk assessment should be event driven or periodic (periodic security review), see also Annex B.

NOTE 4 See also IEC TS 62443-1-1, security level lifecycle.

NOTE 5 Security risk assessment and management is vital in determining exactly what needs to be protected and how this can be achieved.

Figure 2 shows in this context the possible effects of security risk(s) to an SCS.

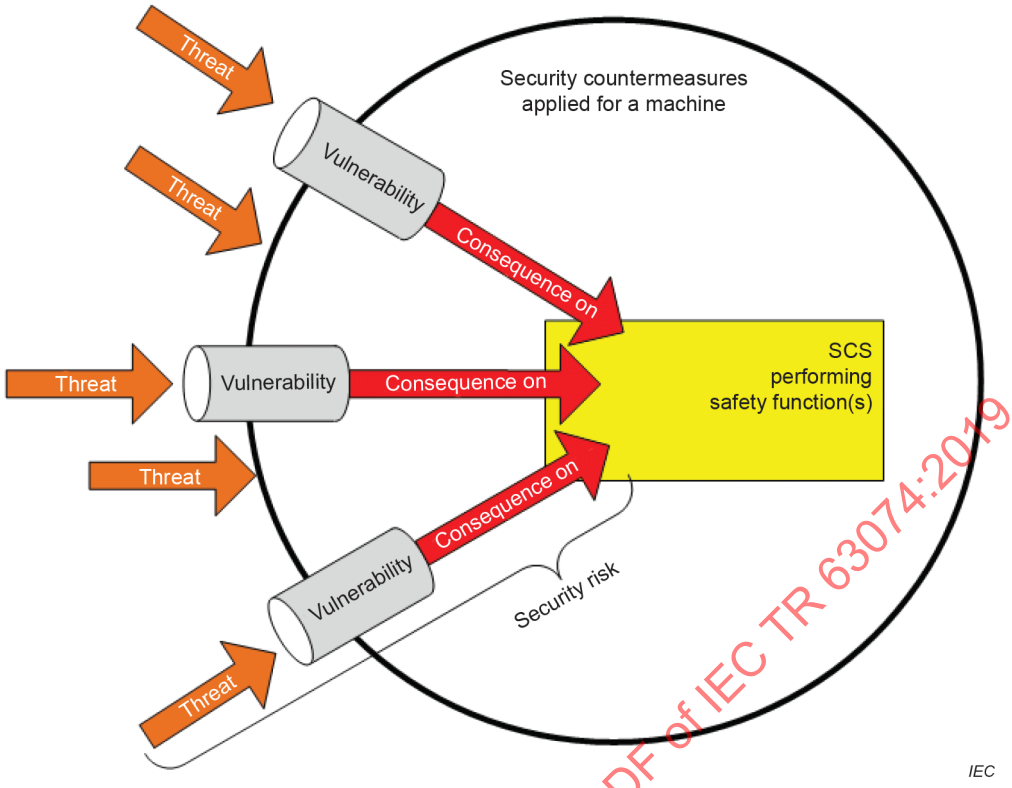


Figure 1 – Relationship between threat(s), vulnerabilities, consequence(s) and security risk(s) for SCS performing safety function(s)

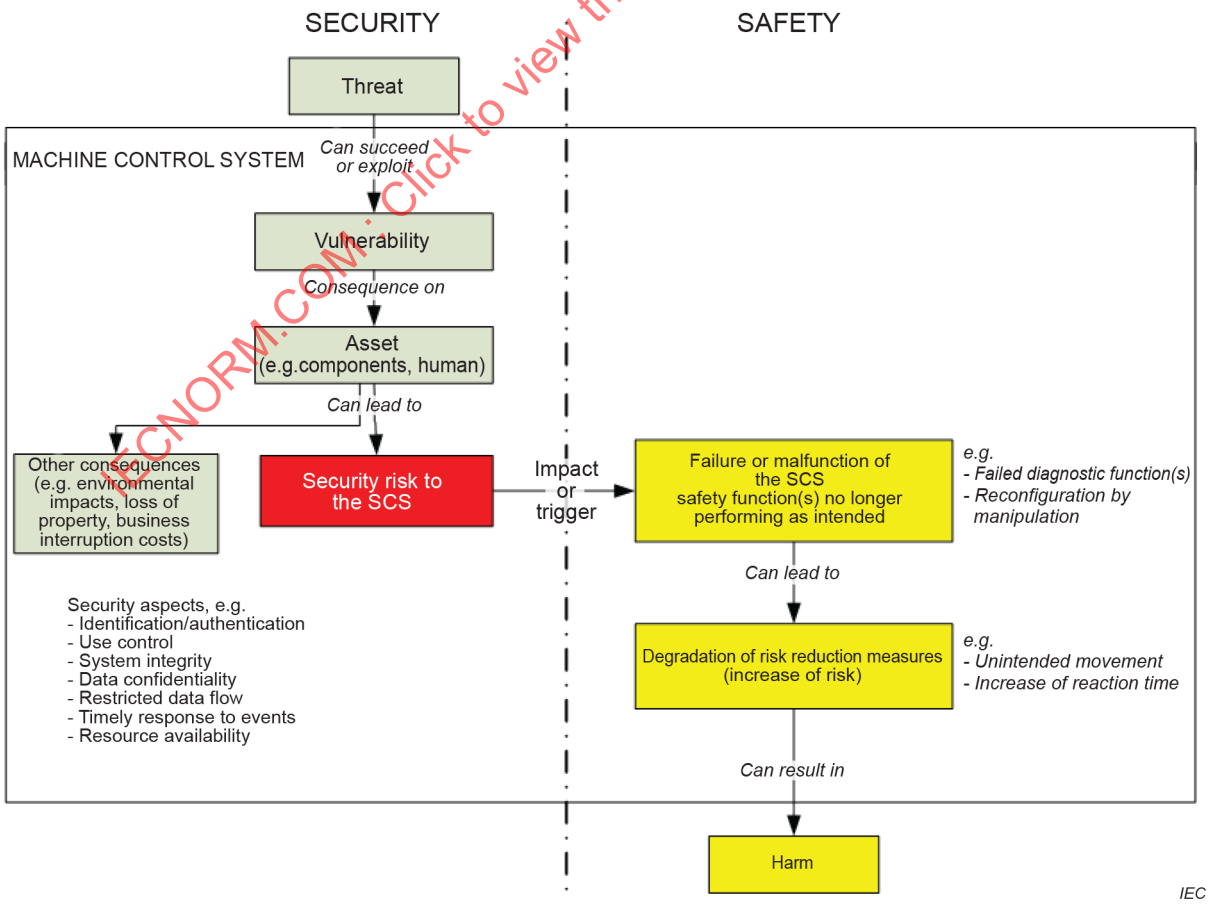


Figure 2 – Possible effects of security risk(s) to a SCS

5 Security aspects related to functional safety

5.1 General

5.1.1 Security risk assessment

NOTE 1 Further information can be found in IEC 62443-2-1 and IEC 62443-3-2.

The security risk assessment relative to SCS is part of the overall security risk assessment of the machine in its environment and includes consideration of various phases such as design, implementation, commissioning, operation, and maintenance.

NOTE 2 The manufacturer of machine usually does not have sufficient information of the machine within its environment to perform the overall security risk assessment, therefore it is typically performed by the combination of the user of the machine and the manufacturer of the machine.

NOTE 3 The implementation or occurrence of "dormant" threats or vulnerability is possible during all lifecycle phases.

NOTE 4 IEC 62443-4-1 recommends for all products an up-to-date threat model with the following characteristics:

– correct flow of categorized information throughout the system;
– trust boundaries;
– processes;
– data stores;
– interacting external entities;
– internal and external communication protocols implemented in the product;
– externally accessible physical ports including debug ports;
– circuit board connections such as JTAG connections or debug headers which might be used to attack the hardware;
– potential attack vectors including attacks on the hardware if applicable;
– potential threats and their severity as defined by a vulnerability scoring system e.g. CVSS (Common Vulnerability Scoring System);
– mitigations and/or dispositions for each threat;
– security-related issues identified;
– external dependencies in the form of drivers or third party applications (code that is not developed by the supplier) that are linked into the application.

A vulnerability assessment is part of a security risk assessment.

Therefore a vulnerability assessment should be carried out to identify vulnerabilities (that can be exploited by threats) of the machine and the potential influence related to safety.

The following information should be available:

a) a description of the devices covered by vulnerability assessment (e.g. mobile panel, or any other device connected to the safety-related control system);

b) a description of identified vulnerabilities that could be exploited by threats and result in security risks;

NOTE 4 Vulnerabilities can be the result of intentional design choices or can be accidental, e.g. resulting from the failure to understand the operational environment.

c) a description of parts of the SCS (e.g. hardware or software) that should be protected by security countermeasures.

The manufacturer of the machine can make some assumption about the threats and implements security countermeasure(s) based on the vulnerability assessment.

NOTE 5 In some cases communication between the manufacturer of the machine and the user of the machine is not possible.

Verification should be performed to ensure that the security countermeasure(s) are appropriate in context of the overall security risk assessment.

NOTE 6 Verification that the security countermeasure(s) are appropriate is normally performed in the machine user environment and can need the information of assumed threats.

Examples of aspects of the security risk assessment are given below:

– identified threats and their sources (including intentional attacks on the hardware, application programs and related software);
– a description of the potential consequences (security risks) resulting from the combination of identified threats and vulnerabilities (see Figure 1);
– the determination of requirements for (additional) measures;

NOTE 7 Additional measures could be adequate safety-related control function(s) to mitigate the consequences of a threat, e.g. safety-related monitoring of limit values, additional security countermeasures, organisational measures, or combination of them.

– a description of, or references to information on the countermeasures taken to reduce or remove the threats.

NOTE 8 A safety-related control system that initially has limited vulnerability can become more vulnerable with situations such as changing environment, changing technology, system failure, unavailability of device replacements, personnel turnover, and greater threat intelligence.

5.1.2 Security risk response strategy

NOTE 1 Further information can be found in IEC TS 62443-1-1:2009, 5.6.4.

NOTE 2 The comparable term to "risk mitigation" is "risk reduction" used in safety of machinery.

Security risk response strategy should be determined during the security risk assessment and taken into consideration in the overall security risk assessment.

Responses to security risks in the field of safety of machinery include:

– mitigate intolerable security risks by
  a) design the security risk out (avoid); or
  b) limit the security risk (e.g. directly by the manufacturer of the machine, or by security countermeasures applied by the user of the machine, or countermeasures shared between the manufacturer and the user of the machine);

NOTE 3 A security risk response strategy could be a defence in depth strategy according to Figure 3 of IEC 62443-4-1:2018.

– accept the security risk if tolerable.

NOTE 4 If the security risk is tolerable no further action is necessary.

5.2 Security countermeasures

5.2.1 General

Any security countermeasure applied for a machine should not adversely affect the safety function performed by the SCS, further investigation has to be performed, e.g. deeper investigation of influences on safety by security countermeasures (e.g. response time of safety function).

NOTE 1 Security countermeasures applied to normal operation functions (machine functions) can have an influence on the safety function performed by the SCS.

Especially the following topics should be considered:

– network architecture;

NOTE 2 Architectural issues relevant to the SCS can be for example:

a) network design (e.g. see zone and conduit model of IEC/TS 62443-1-1:2009, 6.5);
b) firewall configuration;
c) user authorization and authentication;
d) interconnecting different process control networks;
e) wireless communications;
f) access to external networks (i.e., the internet).

– portable devices;
– wireless devices and sensors (this is part of the previous network architecture);
– remote access;
– interfaces to other systems or human machine interfaces.

Annex A gives some information regarding threats that can help to better understand the relationship between threat and vulnerability.

NOTE 3 Security countermeasures can be outside of the machine (e.g. policies procedures and awareness, physical security, network security, computer security and application security).

NOTE 4 The SCS as part of the overall control system can be used to supplement and support security countermeasures.

Security countermeasures should consider the foundational requirements of IEC 62443 (all parts) and possible influences on SCS. Table 1 gives an overview of foundational requirements.

Security countermeasures should also be designed to be scaled to motivation and consequences.

Table 1 – Overview of foundational requirements and possible influence(s) on a SCS

Security foundational requirements	brief description	Safety of Machinery possible influence(s) on a SCS
Identification and authentication control	Identify and authenticate all users (humans, software processes and devices) before allowing them to access to the control system.	Modification or manipulation
Use control	Enforce the assigned privileges of an authenticated user (human, software process or device) to perform the requested action on the control system and monitor the use of these privileges.	Modification or manipulation
System integrity	Ensure the integrity of the control system to prevent unauthorized manipulation.	Influence on safety integrity
Data confidentiality	Ensure the confidentiality of information on communication channels and in data repositories to prevent unauthorized disclosure	Can be relevant for safety
Restricted data flow	Segment the control system via zones and conduits to limit the unnecessary flow of data.	Influence on safety integrity
Timely response to events	Respond to security violations by notifying the proper authority, reporting needed evidence of the violation and taking timely corrective action when incidents are discovered.	Can be relevant for safety integrity
Resource availability	Ensure the availability of the control system against the degradation or denial of essential services.	Influence on availability

NOTE 1 Based on foundational requirements of Subclause 5.3 of IEC TS 62443-1-1:2009 and Annex B of IEC 62443-3-3:2013.

NOTE 2 There is no direct correlation between SIL/PL as defined by IEC 61508, IEC 62061, ISO 13849-1 and SL (Security Level) as defined by IEC 62443-3-3.

5.2.2 Identification and authentication

The capability to identify and authenticate access to the SCS can be necessary.

NOTE 1 Further information can be found in Clause 5 of IEC 62443-3-3:2013.

Examples for preventing unauthorized access and modification are:

– human user identification and authentication;
– authentication for networks;
– account management for software;
– wireless access management;
– password-based authentication;
– password generation and lifetime restrictions for human users;
– identification and authentication procedures between machines.

NOTE 2 Information about authenticator management including use of default passwords can be found in Subclause 5.7.2 of IEC 62443-3-3:2013.

5.2.3 Use control

When a user is identified and authenticated, it can be necessary that the SCS restrict the allowed actions to the authorized use of the SCS (assigned privileges of an authenticated user).

NOTE Further information can be found in Clause 6 of IEC 62443-3-3:2013.

5.2.4 System integrity

The user of the machine(s) (e.g. asset owner) is typically involved in maintaining the system integrity of the control system (including the SCS) to prevent unauthorized manipulation.

NOTE 1 Maintenance of system integrity is based on security risk assessment; information about triggers can be found in Annex B.

NOTE 2 Further information can be found in Clause 7 of IEC 62443-3-3:2013.

Therefore the following aspects can be relevant:

– communication integrity/corruption (LAN, WLAN, etc.), e.g. using of cryptographic integrity protection in untrusted networks;
– malicious code protection (against manipulation, for example, viruses, worms, Trojan horses and spyware), e.g. by consideration of concerned interfaces (e.g. USB, programming interface for PLC or SCS);
– software and information integrity (unauthorized changes);
– input validation (rules for checking the input data, out-of-range values);

5.2.5 Data confidentiality

In general, some control system-generated information, whether at rest or in transit, is of a confidential or sensitive nature. This implies that some communication channels and stored data require protection against eavesdropping and unauthorized access.

NOTE Further information can be found in Clause 8 of IEC 62443-3-3:2013.

In the context of control system(s), this aspect can be relevant for safety, e.g. unauthorized access to a database providing identifications and privileges of authorized people.

5.2.6 Restricted data flow

Any requirements for information flow restrictions will be determined by the overall security risk assessment.

NOTE Further information can be found in Clause 9 of IEC 62443-3-3:2013.

Transmission delay or increased response time can influence the safety integrity of an SCS (e.g. configuration of network).

5.2.7 Timely response to events

The user of the machine(s) (e.g. asset owner) should establish security policies and procedures and proper lines of communication and control needed to timely respond to security violations.

NOTE Further information can be found in Clause 10 of IEC 62443-3-3:2013.

This aspect will be considered in the overall security risk assessment and can be relevant for the safety integrity of an SCS.

5.2.8 Resource availability

The aim is to ensure that the control system is resilient against various types of denial of service events.

NOTE Further information can be found in Clause 11 of IEC 62443-3-3:2013.

This aspect will be considered in the overall security risk assessment.

Transmission delay or increased response time can influence the availability of an SCS.

6 Verification and maintenance of security countermeasures

The implementation of the security countermeasures should be verified and maintained by the user of the machine(s), the manufacturer of the machine and the subsystem manufacturer as appropriate (see also security risk assessment, 5.1.1).

NOTE Verification can be achieved by testing or analysis.

7 Information for the user of the machine(s)

The manufacturer of the machine should provide information to the user of the machine(s) in order to support the overall security risk assessment.

This typically can include:

– summary of safety functions (architecture, network topology, etc.);

NOTE 1 This can include prerequisites for security countermeasures to avoid degradation of safety function performed by SCS (see 5.2).

– information based on vulnerability assessment (see 5.1.1) or on identified or reported vulnerabilities, where appropriate;

– information about security countermeasures already implemented within the machine (see 5.2), where appropriate.

NOTE 2 Information about initial exchange and updating of information is provided in Annex B and Annex C.

Annex A
(informative)

Basic information related to threats and threat modelling approach

A.1 Evaluation of threats

Threats can be described as the possible actions that can be taken against a system. Types of threats can be accidental or non-validated changes.

Threats to assets can result from inadvertent events as well as deliberate attacks.

Threat agent is the term used to describe the entity that presents a threat. They are also known as adversaries or attackers.

Ultimately no protection against attacks, failures, mistakes, or natural disasters can ever be completely absolute.

Threat agents can be defined as one of the following:

– Malicious person (malicious) who is deliberately attacking systems for financial, power, revenge, or other gain
  - 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."
  - 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.
– Inadvertent mistake (error) caused by a person who either failed to pay attention or did not recognize the consequences of their action. Computer applications can also have "bugs" or other flaws that cause them to mis-operate. Poorly designed systems and inadequate operating procedures also fall In this category.
– Equipment failure (failure) that was not any person's fault, but reflects the fact that electronic and mechanical devices can fail. Equipment that responds in unexpected ways to normal conditions can also be placed in this category.
– Natural disasters (disaster) caused by events completely outside the control of humans.

Threats may be either passive or active.

– Passive – Threat agents usually gather passive information by casual verbal communications with employees and contractors
– Active – Examples are:
  - Communication: The intent of a communication attack is to disrupt communications for control systems;
  - Database injection: Injection attacks are used to steal information from a database or to corrupt data integrity of a database;
  - Replay: Signals may be captured from control system communications paths and replayed later to provide access to secured systems or to falsify data in a control system;
  - Spoofing and impersonation: In networking, the term is used to describe a variety of ways in which hardware and software can be fooled;
  - Social engineering: Threat agents also obtain or attempt to obtain otherwise secure data by tricking an individual into revealing secure information;

- Phishing: Phishing relies on social engineering in that humans tend to believe in the security of a brand name, associating it with trustworthiness;
- Malicious code: Malicious code attacks can take the form of viruses, worms, automated exploits, or Trojan Horses;
- Denial of service (DoS): Denial (or degradation) of service attacks affect the availability of a network, operating system, or application resources;
- Escalation of privileges: With these increased privileges the attacker can take actions that would otherwise be prevented;
- 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 control system.

NOTE Further information on threats can be found in 5.6.5 of IEC TS 62443-1-1:2009.

A.2 Examples of threat related to a safety-related device

Consideration should be given to a possible attack scenario that can influence the safety function(s) performed by a SCS, using one or several safety-related devices.

Possible access to the devices comprising of the SCS by any person with malicious intent should be considered. A deliberate (human) attack represents a threat to take control of a safety-related device. This attack can occur directly to the safety-related device by, for example:

– an interactive screen or control panel;
– switches or buttons for device configuration or
– configuration or program stored in a memory, e.g. removable SD card.

NOTE The above is just intended as an indicative list. There are many other possible vulnerabilities to direct attack including tools given by a manufacturer to configure a safety-related control system.

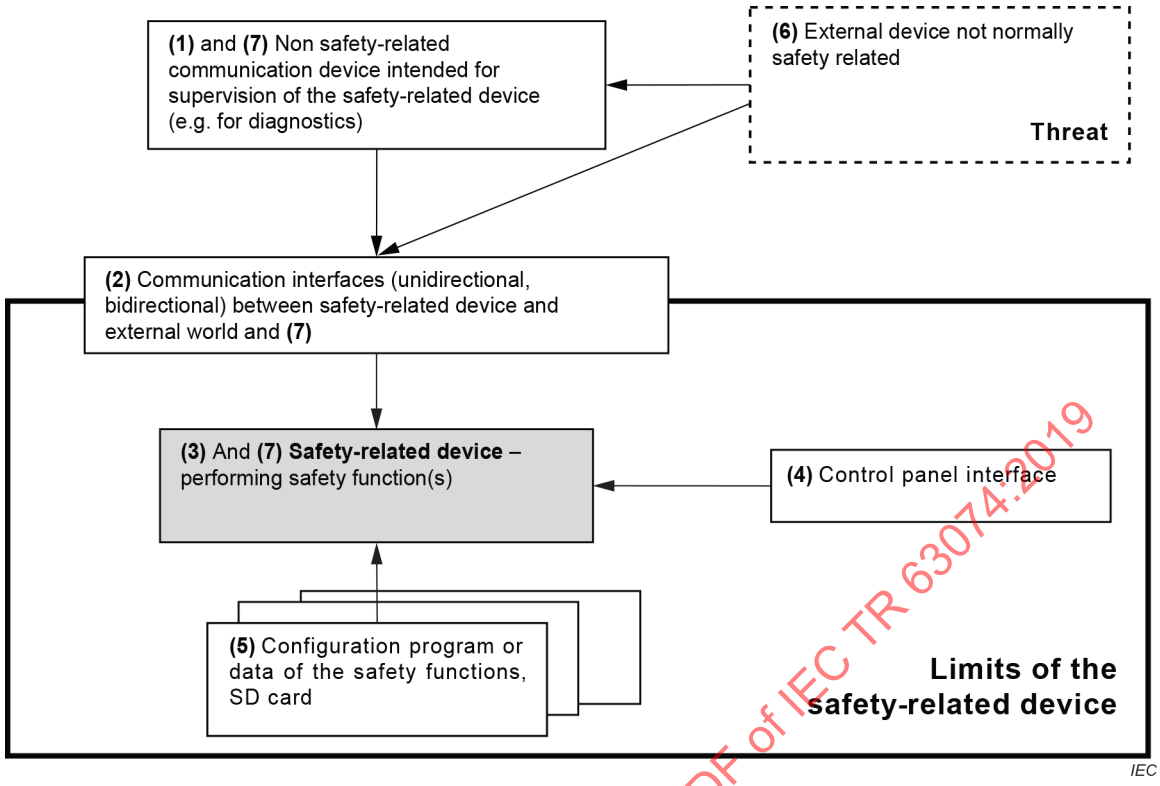
An attack can occur indirectly to the safety-related device, for example by:

– computer technology;
– network communication technology or
– wireless communication technology.

In these three cases the access to the safety-related device is gained indirectly by using other technologies. Attacks are well known in computer technologies.

The vulnerability of the security of a safety-related device is linked to the technologies used for its access. The security countermeasures should be based on the "weak points" of each technology.

Figure A.1 shows an example of vulnerability where a safety function could be altered due to a threat.



At each level, where the access to the safety function is possible, different measures are necessary, for example:

Level	Notes
1)	The communication from a supervisory device to the safety-related device can introduce vulnerabilities. An attack on the safety-related device or a failure of the supervisory device may allow unauthorised access to the safety function.
2)	The communication from the safety-related device to the supervision is in most cases done through a coupler communication. The choice of a unidirectional coupler (from the safety-related device to the supervision) can limit the access from the attack to the safety function. This kind of technology is the same as used for servers and networks. The faults are well known and well-tried protection measures against hacking are put in place.
3)	Safety-related device performing safety function(s).
4)	A control panel can have access to devices implementing the safety function. Different levels of password protection for different access privileges can reduce the vulnerability.
5)	On some safety-related devices configuration is done with switches or SD memory. An attack can consist of a change of the switches or the SD card that contains the configuration program. So countermeasures need to be implemented.
6)	A portable external device not normally connected can have access to the safety related device through the communication interface or communication device. In this case it is a threat that is similar to the one described on **(2)**.
7)	Linked to **(6)** an attack can consist of a program being put inside the communication interface, that can control the safety device on request – examples of this type of attack on the DNS servers are known.

Figure A.1 –Safety-related device and possible accesses