IEC TS 63074

Edition 1.0 2023-02

TECHNICAL SPECIFICATION

colour inside

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

IEC TS 63074:2023-02(en)

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

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

IEC TS 63074

Edition 1.0 2023-02

TECHNICAL SPECIFICATION

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 978-2-8322-6468-3

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

CONTENTS

FOREWORD 4
INTRODUCTION 6
1 Scope 7
2 Normative references 7
3 Terms, definitions, and abbreviated terms 8
3.1 Terms and definitions 8
3.2 Abbreviated terms 12
4 Safety and security overview 12
4.1 General 12
4.2 Safety objectives 12
4.3 Security objectives 13
5 Security aspects related to functional safety 15
5.1 General 15
5.1.1 Security risk assessment 15
5.1.2 Security risk response strategy 16
5.2 Security countermeasures 16
5.2.1 General 16
5.2.2 Identification and authentication 18
5.2.3 Use control 18
5.2.4 System integrity 18
5.2.5 Data confidentiality 18
5.2.6 Restricted data flow 19
5.2.7 Timely response to events 19
5.2.8 Resource availability 19
6 Cybersecurity and functional safety of machinery 19
6.1 General 19
6.2 Aspects related to the protection against corruption 19
6.3 Security countermeasures against corruption 20
6.3.1 General 20
6.3.2 Potential sources of cyber threats 20
6.3.3 Multi-factor authentication 20
6.3.4 Network architecture 20
6.3.5 Portable devices 21
6.3.6 Wireless communication 21
6.3.7 Remote access 21
6.3.8 Attack through direct physical connection 22
7 Verification and maintenance of security countermeasures 22
8 Information for the user of the machine(s) 22
Annex A (informative) Basic information related to threats and threat modelling approach 23
A.1 Evaluation of threats 23
A.2 Examples of threat related to a safety-related device 24
Annex B (informative) Security risk assessment triggers 26
B.1 General 26
B.2 Event driven triggers 26

Annex C (informative) Example of information flow between device supplier, manufacturer of machine, integrator and user of machine 27
C.1 General....27
C.2 Example 1 – Design phase of the machine....27
C.3 Example 2 – Use phase of the machine 27
Bibliography....29

Figure 1 – Relationship between threat(s), vulnerabilities, consequence(s) and security risk(s) for SCS performing safety function(s)....14
Figure 2 – Possible effects of security risk(s) to an SCS 14
Figure A.1 – Safety-related device and possible accesses 25
Figure C.1 – Example of generic information flow during design phase 27
Figure C.2 – Example of generic information flow during use phase....28
Figure C.3 – Example of information flow during use phase in context of IEC 62443-2-4....28

Table 1 – Overview of foundational requirements and possible influence(s) on an SCS 17

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.

IEC TS 63074 has been prepared by IEC technical committee 44: Safety of machinery – Electrotechnical aspects. It is a Technical Specification.

This first edition cancels and replaces the first edition of IEC TR 63074 published in 2019. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to IEC TR 63074:2019:

a) new Clause 6 on Cybersecurity and functional safety of machinery;

b) new Figure A.1;

c) new Clause C.3 Example 2 – Use phase of the machine.

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

Draft	Report on voting
44/964/DTS	44/987/RVDTS

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this Technical Specification is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/standardsdev/publications.

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.

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 threats exploiting vulnerabilities due to the fact that:

- access to the control system is possible, for example re-programming of machine functions (including safety);
- "convergence" between standard IT and industrial systems is increasing;
- operating systems have become present in embedded systems, for example 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 for example unauthorized access, availability and integrity.

In the context of the machine, the machine control system represents an industrial automation system.

The safety-related control system of machines is part of the machine control system and can therefore also be subject to security threats 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 due to 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 will 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) in accordance with IEC 62061 for safety-related control systems or the IEC 61508 series for electrical/electronic/programmable electronic safety-related systems, or the Performance Level (PL) in accordance with ISO 13849-1 for safety-related parts of control systems).

With respect to the safety function, the security threats (internal or external) can 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 document; further information is provided for example in the IEC 62443 series or ISO/IEC 27001.

Measures to prevent reasonably foreseeable misuse by physical manipulation are addressed in some machinery functional safety standards (e.g. the IEC 61496 series and ISO 14119).

NOTE 4 Measures to prevent reasonably foreseeable misuse by physical manipulation are not the same as physical security in the IEC 62443 series.

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

1 Scope

This technical specification identifies the relevant aspects of the IEC 62443 series related to security threats and vulnerabilities that are considered for the design and implementation of safety-related control systems (SCS) which can lead to the loss of the ability to maintain safe operation of a machine.

Typical security aspects related to 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.

Non-safety-related aspects of security threats and vulnerabilities are not considered in this document.

NOTE Non-safety-related parts of the machine control system can also be affected by security threats with possible impact on operation of a machine, such as productivity, performance or quality. For these aspects, refer to the IEC 62443 series.

The focus of this document is on intentional malicious actions. However, intentional hardware manipulation (e.g. wiring, exchange of components) or foreseeable misuse by physical manipulation of SCS (e.g. physical bypass) is not considered in this document.

This document does not cover security requirements for information technology (IT) products and for the design of devices used in the SCS (e.g., product specific standards can be available, such as IEC TS 63208).

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 62061:2021, *Safety of machinery – Functional safety of safety-related control systems*

3 Terms, definitions, and abbreviated terms

3.1 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

[SOURCE: IEC TS 62443-1-1:2009, 3.2.16, modified – Notes deleted]

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
machine control system
system that responds to input signals from the machine, a process and/or from an operator and generates output signals causing the machine to operate in the desired manner

Note 1 to entry: The machine control system includes input and output devices, including sensors and actuators.

Note 2 to entry: “Signals” can also be data.

[SOURCE: IEC 61508-4:2010, 3.3.3, modified – The term defined has been changed, "process" has been changed to "machine", Note to entry amended and Note 2 to entry added]

3.1.6
cybersecurity
<of the machine control system> set of activities necessary to protect network and information systems of the machine control system, the users of such systems, and other persons from cyber threats, typically regarding the aspects of confidentiality, integrity and availability

3.1.7
cyber threat
<of the machine control system> potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons, typically exploiting vulnerabilities of a machine system

3.1.8
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 – in item a) “EUC” has been replaced by "machine"]

3.1.9
functional safety
part of the overall safety relating to the machine and the machine control system that depends on the correct functioning of the safety-related control systems and other risk reduction measures

[SOURCE: IEC 61508-4:2010, 3.1.12, modified – "EUC" replaced by "machine", "E/E/PE safety-related systems" replaced by “safety-related control systems”]

3.1.10
integrator
entity who designs, manufactures or assembles an integrated manufacturing system and is responsible for the safety strategy, including the protective measures, control interfaces and interconnections of the control system

Note 1 to entry: The integrator may be for example a manufacturer, assembler, engineering company, or entity with the overall responsibility for the machine.

[SOURCE: IEC 62061:2021, 3.2.13]

3.1.11
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 12100:2010, 3.1, modified – removal of Note 2]

3.1.12
network and information systems
<of the machine control system> means or devices that contribute to or participate in the transmission or exchange of data

Note 1 to entry: Network and information systems can be:

a) an electronic communications network within the meaning of transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, radio, optical or other electromagnetic means used for a machine;

b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or

c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance.

3.1.13
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]

3.1.14
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO 12100:2010, 3.12]

3.1.15
safety
freedom from risk which is not tolerable

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

3.1.16
safety function
function of a machine whose failure can result in an immediate increase of the risk(s)

[SOURCE: ISO 12100:2010, 3.30]

3.1.17
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]

3.1.18
safety-related control system
SCS
part of the control system of a machine which implements a safety function by one or more subsystems

[SOURCE: IEC 62061, 3.2.3, modified – Note 1 to entry omitted]

3.1.19
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 a machinery and its 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, modified – in item e) “industrial automation and control system” replaced by “a machinery and its control system”]

3.1.20
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]

3.1.21
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 – in the term, "risk" replaced by "security risk"]

3.1.22
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" in the term, "total exposure" replaced by "the exposure", removal of Notes.]

3.1.23
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]

3.1.24
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]

3.1.25
user of the machine
entity with the overall responsibility for the use of the machine

3.1.26
vulnerability
<of the machine control system> weakness of a machine control system or a countermeasure that can be exploited by one or more threats to violate the machine control system's integrity

3.1.27
vulnerability assessment
formal description and evaluation of the vulnerabilities in a system

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

3.2 Abbreviated terms

CVSS	common vulnerability scoring system
DoS	denial of service
IT	information technology
JTAG	joint test action group
LAN	local area network
PL	performance level
PLC	programmable logic controller
SCS	safety-related control system
SD	secure digital
SIL	safety integrity level
USB	universal serial bus
VPN	virtual private network
WLAN	wireless local area network

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) (including safety-related data).

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 risk assessment which can be performed in accordance with ISO 12100 and where available, 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 functions that are performed by an SCS achieve a safety integrity which is quantifiable as SIL in accordance with IEC 62061 for safety-related control systems (or the IEC 61508 series for electrical/electronic/programmable electronic safety-related systems) or PL in accordance with ISO 13849-1 for safety-related parts of control systems.

4.3 Security objectives

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

NOTE 1 Security objectives are for example:

- availability of machine(s), including safety functions;
- integrity against manipulations;
- confidentiality by means of methods commonly accepted by both the security and industrial automation communities;
- 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.

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 or system in its environment on which threats and known vulnerabilities are identified. 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 IEC TS 62443-1-1:2009, 5.5.

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 shall not adversely affect any safety function (see Figure 1).

NOTE 3 Essential functions in accordance with 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: 2009, 5.12, security level lifecycle.

NOTE 5 Security risk assessment and management are vital in determining exactly what will be protected and how this can be achieved.

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

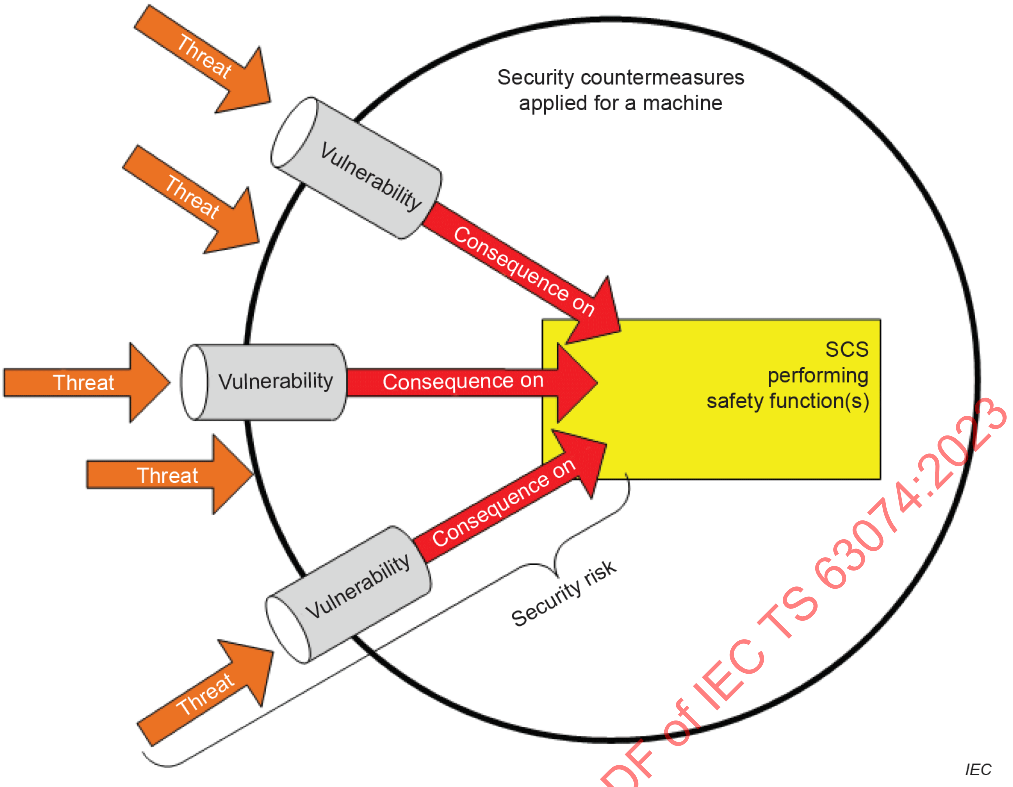


Figure 1 – Relationship between threat(s), vulnerabilities, consequence(s) and security risk(s) for SCS performing safety function(s)

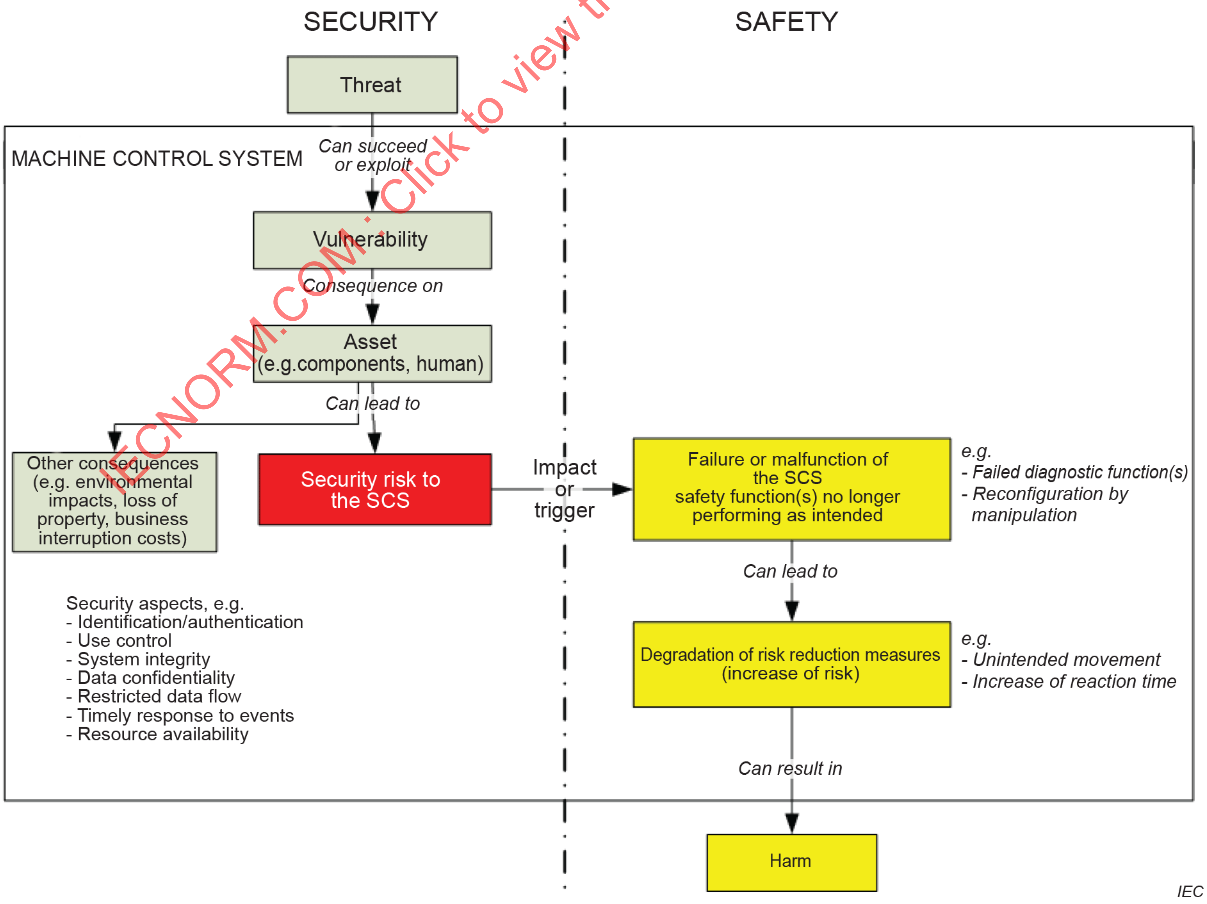

SECURITY
SAFETY
Threat
MACHINE CONTROL SYSTEM
Can succeed or exploit
Vulnerability
Consequence on
Asset (e.g.components, human)
Can lead to
Other consequences (e.g. environmental impacts, loss of property, business interruption costs)
Security risk to the SCS
Impact or trigger
Failure or malfunction of the SCS safety function(s) no longer performing as intended
e.g.
- Failed diagnostic function(s)
- Reconfiguration by manipulation
Can lead to
Degradation of risk reduction measures (increase of risk)
e.g.
- Unintended movement
- Increase of reaction time
Can result in
Harm
Security aspects, e.g.
- Identification/authentication
- Use control
- System integrity
- Data confidentiality
- Restricted data flow
- Timely response to events
- Resource availability
IEC

Figure 2 – Possible effects of security risk(s) to an 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 an 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 the machine usually does not have sufficient information on 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 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, for example common vulnerability scoring system (CVSS);
- mitigations or dispositions for each threat, or both;
- 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.

As part of the security risk assessment, a vulnerability assessment shall 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 shall be available:

- a description of the devices covered by the vulnerability assessment (e.g. mobile panel, or any other device connected to the safety-related control system);
- a description of identified vulnerabilities that can be exploited by threats and result in security risks;

  NOTE 4 Vulnerabilities can be the result of intentional design choices or can be accidental, for example resulting from the failure to understand the operational environment.
- 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 in consideration of the foreseen machine installation site and implements security countermeasure(s) based on the vulnerability assessment.

NOTE 5 Communication between the manufacturer of the machine and the user, where possible, can address these assumptions.

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

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

Examples of aspects of the security risk assessment are given as follows:

- 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 can be adequate safety-related control function(s) to mitigate the consequences of a threat, for example safety-related monitoring of limit values, additional security countermeasures, organisational measures, or a 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 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:

a) mitigating intolerable security risks by

   - avoiding the security risk by design; or
   - limiting 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 2 A security risk response strategy can be a defence in depth strategy in accordance with IEC 62443-4-1:2018, Figure 3.

b) accepting the security risk if tolerable.

NOTE 3 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 shall not adversely affect the safety function performed by the SCS, and further investigation has to be performed, for example 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 shall be considered:

- network architecture;

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

  - network design (e.g. see the zone and conduit model of IEC TS 62443-1-1:2009, 6.5);
  - firewall configuration;
  - user authorization and authentication;
  - interconnecting different process control networks;
  - wireless communications;

  - 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 engineering software tools (including engineering environment);
- 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 implemented outside of the machine by the user 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, when relevant.

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

Security countermeasures should also be designed to be appropriate for motivation and consequences.

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

Security foundational requirements	Brief description	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.	Influence on safety integrity by 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.	Influence on safety integrity by 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.	Possible indirect influence on safety integrity (e.g. inaccessible information on the safety configuration).
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.	Possible indirect influence on safety integrity (e.g. by ignoring security violations that prevent the application of the appropriate counter measures).
Resource availability	Ensure the availability of the control system against the degradation or denial of essential services.	Influence on availability.
NOTE 1 Based on the foundational requirements of IEC TS 62443-1-1:2009, 5.3, and of IEC 62443-3-3:2013, Annex B. NOTE 2 There is no direct correlation between SIL or 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 IEC 62443-3-3:2013, Clause 5.

NOTE 2 5.2.2 is also applicable to engineering software tools (including engineering environment).

Examples for preventing unauthorized access and modification are:

- measures preventing the physical access to the control system of the SCS, for example locking of the enclosure;
- 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 3 Information about authenticator management including use of default passwords can be found in IEC 62443-3-3:2013, 5.7.2.

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 IEC 62443-3-3:2013, Clause 6.

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 the system integrity is based on a security risk assessment; information about triggers can be found in Annex B.

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

Therefore the following aspects can be relevant:

- communication integrity or corruption (LAN, WLAN, etc.), or both, for example use of cryptographic integrity protection in untrustworthy networks;
- malicious code protection (against manipulation, for example, viruses, worms, Trojan horses and spyware), for example 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 IEC 62443-3-3:2013, Clause 8.

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) and should be prevented.

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 IEC 62443-3-3:2013, Clause 9.

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

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 respond quickly to security events.

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

This aspect will be considered in the overall security risk assessment and can have a possible indirect influence on safety integrity.

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 IEC 62443-3-3:2013, Clause 11.

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

Transmission delay or increased response time can influence the availability of an SCS and should be prevented

6 Cybersecurity and functional safety of machinery

6.1 General

In view of addressing the risks related to new digital technologies, stemming from malicious actions provoked by a third-party and having an impact on the safety of machinery, manufacturers shall consider proportionate security countermeasures which are limited to the protection of the machine control system.

6.2 Aspects related to the protection against corruption

Corruption of data or information poses an important vulnerability to network and information systems, for example connections between devices. The security risk assessment relative to SCS shall include the following aspects in the context of the use of the machinery and network and information systems:

- Connection to safety-related devices (as subsystems or subsystem elements of SCS) and another device, via any feature of the connected device itself or via any remote device that communicates with those safety-related devices, shall not lead to the degradation of the safety integrity of the SCS and shall not lead to a hazardous situation.
- The hardware component for data connection that is critical for the safety integrity of an SCS shall be analysed so that it is adequately protected against intentional corruption.

- Software and data that are critical for the SCS to perform its intended safety function shall be identified as such and shall be adequately protected against intentional corruption.
- Safety-related software shall be identified and this information should be provided in an easily accessible form, where appropriate.
- Modification of the safety-related software on the machinery or its configuration shall be recorded.

6.3 Security countermeasures against corruption

6.3.1 General

The following typical devices and human actions shall be analysed to provide adequate security countermeasures and identify potential vulnerabilities regarding the use of machinery (see Clause 5 and Figure A.1).

A software update should be considered where appropriate.

6.3.2 Potential sources of cyber threats

Based on the security risk assessment potential sources of cyber threats, including but not limited to the following aspects (or vulnerabilities), shall be considered and analysed for further investigation:

- network architecture;
- portable devices;
- wireless devices and sensors;
- remote access;
- interfaces to other systems or human machine interfaces.

6.3.3 Multi-factor authentication

6.3.3.1 General

Where any kind of human interaction with the SCS or parts of it is necessary, a multi-factor authentication shall be considered if possible corruption of data can lead to the degradation of the safety integrity of the SCS.

NOTE Depending on the security risk assessment the two security factors can use either different devices or the same device.

EXAMPLE: Safety-related parameters will be changed by the operator of the machinery.

6.3.3.2 Basic approach

Based on the information provided or used by the operator of a machinery, the security factors shall be stored and used in such a way that a single attack on the user environment does not lead to multiple factors being compromised. Instructions to the operator of a machinery to handle the factors in an appropriately secure manner shall also be considered.

The two security factors shall use either different transmission paths or different transmission data. These requirements can be fulfilled by transmitting the two factors separately in time on the same transmission path, provided that it is ensured that the first factor has been transmitted and received before the second will be transmitted.

NOTE Another approach can also be the separation of transmission channels or data.

6.3.4 Network architecture

As a result of security risk assessment, a division of the network architecture into zones can be carried out. Safety-related devices and data (or information) with similar protection requirements should be combined. This combination has many advantages if security countermeasures are implemented to derive network segmentation, for example by firewalls. If a zone fails, for example due to a hacker attack, a virus or internal manipulation, other zones are not affected and the SCS continues to operate uninfluenced.

This network segmentation shall be regularly checked to verify that it is up-to-date and effective.

6.3.5 Portable devices

Any human interaction resulting from using portable devices shall be analysed regarding the implication with any SCS. Where safety-related communication is used, security countermeasures such as multi-factor authentication should be applied.

6.3.6 Wireless communication

In the industrial environment, wireless communication, for example via tablets, laptops, etc., is becoming increasingly popular. It usually takes place via WLAN (wireless local area network) or Bluetooth®[1]. The standard passwords of the device manufacturers are often already publicly known after a short time. A change of the standard passwords with sufficient length is indispensable. The wireless communication coverage distance should not be longer than necessary.

Where safety-related communication is used security countermeasures shall be considered, for example by using cryptography provided by a commonly accepted security protocol. As additional measure, multi-factor authentication can also be of interest for this purpose.

NOTE Information about requirements for cableless control systems of machinery can be found in IEC 62745.

6.3.7 Remote access

Remote access can be relevant, for example for maintenance, and can have implications on SCS.

EXAMPLE: During the remote maintenance of machines and plants, data is transmitted between the operator and the manufacturer via the Internet. If no precautions are taken, this results in several weak points with regard to security. Authentication and authorization mechanisms become important. This can be achieved, for example, by manually enabling the required port for remote maintenance or by a separate cable connection to the machine.

The transmission of data via network and information systems shall be considered where data can be intercepted by third parties. For this purpose, security countermeasures such as the implementation of a virtual private network (VPN) connection and multi-factor authentication can be implemented.

NOTE 1 The advantage is that this end-to-end encryption means that only authorized senders and receivers can read the data. Any "interception" of the data anywhere in network and information systems is worthless because the information is encrypted.

NOTE 2 Internet, WLAN, Bluetooth, etc. can be subject to remote attacks without physical access to the safety-related control system.

Time-limited remote access to a machine, for example by disabling the connection after a predefined time frame, should be considered as a measure to limit the possibility of malicious access.

In order to avoid a malicious remote access to a machine from compromising SCS, modification to safety-related parameters can be locally confirmed.

[1] Bluetooth® is an example of suitable product available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of this product.

6.3.8 Attack through direct physical connection

Direct physical connection to the safety related control system can be relevant and can have implications on SCS. Typical examples are an SD card, USB, network ports (e.g. ethernet, RS 485), JTAG, etc. (see Figure A.1, measures (4) and (5)).

Unused ports of the machine control system (e.g., USB ports, network ports, etc.) should be disabled to minimize the possibility of unauthorized malicious access.

7 Verification and maintenance of security countermeasures

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

NOTE 1 Verification can be achieved by testing or analysis.

NOTE 2 Maintenance of security countermeasures can include, for example, software patches, firmware updates, replacement of hardware components, additional countermeasures or changing of already implemented countermeasures.

8 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:

- the foreseen machine installation site;
- 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 (see Clause 6), 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.

NOTE 3 Additional information about the information for the use of the machine can be found in ISO/TR 22100-4:2018, 10.4.

Information on replacement, decommissioning or disposal of the machine control system shall be provided to ensure that there is no negative impact on the (cyber) security countermeasures of the SCS: Replacement, decommissioning or disposal of the machine control system or its IT environment shall be done in such a way that there is no loss of confidentiality of information (e.g. stored passwords on a memory chip in e-waste) and no disruptive impact on the (cyber) security countermeasures of the SCS still in operation.

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 for example against a system. Types of threats can be accidental or non-validated changes.

NOTE 1 Threats can be facilitated if the changes are not validated.

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

Threat agents is the term used to describe the entities that present 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:

a) A malicious person who is deliberately attacking systems for financial reward, 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 can 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 can be known, or not, to the targeted organization. Outsiders can have been insiders, or not, at one time.

b) 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.

c) Equipment failure (failure) that was not any person’s fault, but reflects the fact that electronic and mechanical devices fail in preventing the threat from having success.

d) Natural disasters (disaster) caused by events completely outside the control of humans.

Threats can be either passive or active.

1) Passive – Threat agents usually gather passive information by casual verbal communications with employees and contractors.

2) 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 can 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 2 Further information on threats can be found in IEC TS 62443-1-1:2009, 5.6.5.

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 an SCS, using one or several safety-related devices.

Possible access to the devices comprising 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 against the safety-related device by, for example:

– an interactive screen or control panel;

– non-safety-related parts (e.g. web server integrated into the safety-related device);

– switches or buttons for device configuration; or

– configuration or program stored in a memory, for example 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.

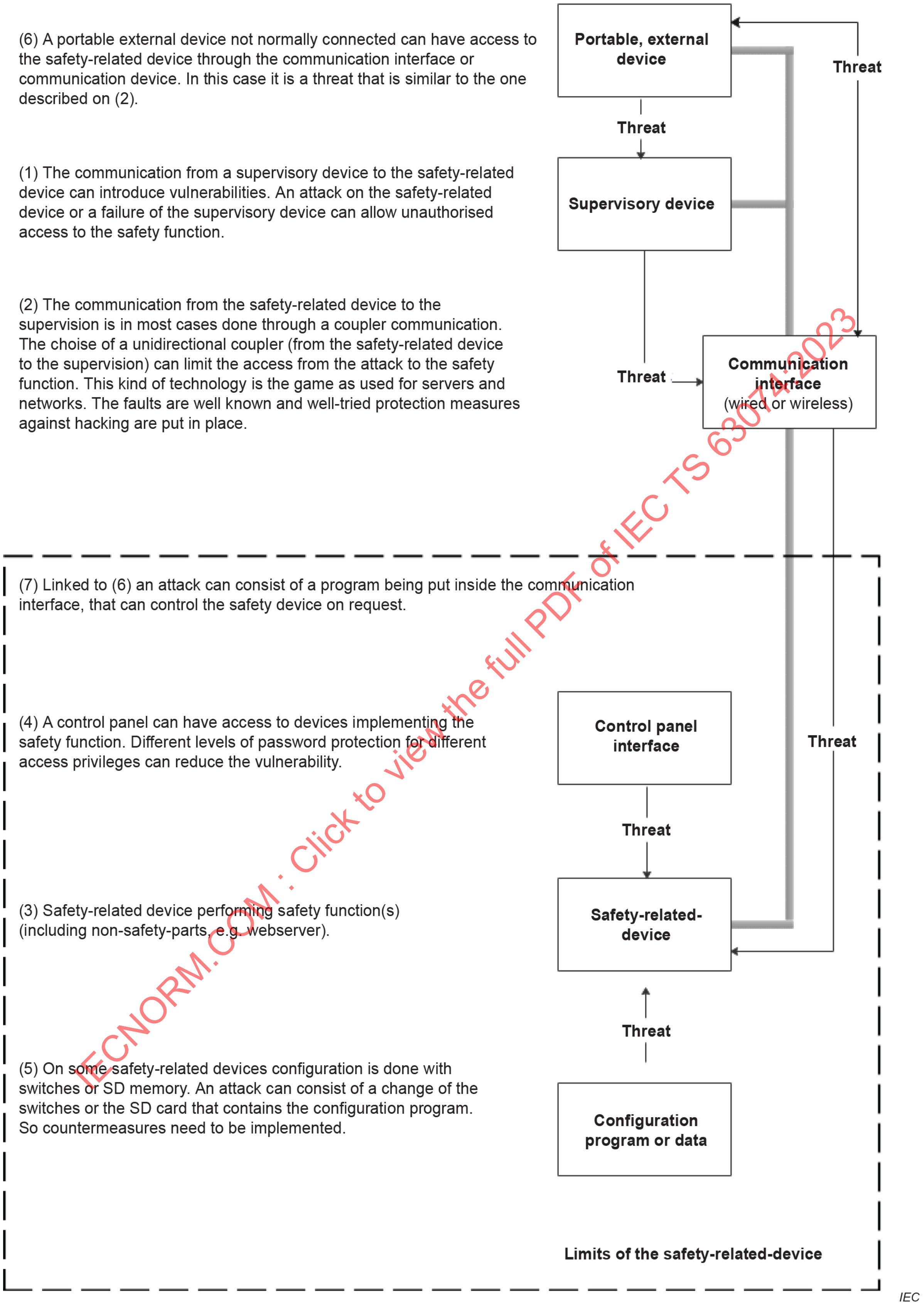
An attack can occur indirectly against the safety-related device, for example by:

1) computer technology;
2) network communication technology or
3) 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 can be altered due to a threat. For each item, where the access to the safety function is possible, different measures are necessary.



(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).

(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 can 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 choise 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 game as used for servers and networks. The faults are well known and well-tried protection measures against hacking are put in place.

(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.

(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.

(3) Safety-related device performing safety function(s) (including non-safety-parts, e.g. webserver).

(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.

Portable, external device
Threat
Threat
Supervisory device
Threat
Communication interface (wired or wireless)
Control panel interface
Threat
Threat
Safety-related-device
Threat
Configuration program or data
Limits of the safety-related-device
IEC

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