44/764/NP

NEW WORK ITEM PROPOSAL

	Proposer GERMANY	Date of proposal 2016-04
	TC/SC 44	Secretariat UK
	Date of circulation 2016-04-15	Closing date for voting 2016-07-08

A proposal for a new work item within the scope of an existing technical committee or subcommittee shall be submitted to the Central Office. The proposal will be distributed to the P-members of the technical committee or subcommittee for voting on the introduction of it into the work programme, and to the O-members for information. The proposer may be a National Committee of the IEC, the secretariat itself, another technical committee or subcommittee, an organization in liaison, the Standardization Management Board or one of the advisory committees, or the General Secretary. Guidelines for proposing and justifying a new work item are given in ISO/IEC Directives, Part 1, Annex C (see extract overleaf). **This form is not to be used for amendments or revisions to existing publications.**

The proposal (to be completed by the proposer)

Title of proposal

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

☒ Standard	□ Technical Specification

Scope (as defined in ISO/IEC Directives, Part 2, 6.2.1)

This International Standard considers aspects of security threats and vulnerabilities that may lead to the loss of the ability to maintain safe operation of a machine (safety measures) related to safety-related control systems.

Purpose and justification, including the market relevance, whether it is a proposed horizontal standard (Guide 108)[1] and relationship to Safety (Guide 104), EMC (Guide 107), Environmental aspects (Guide 109) and Quality assurance (Guide 102) . (attach a separate page as annex, if necessary)

The IEC 62443series of IEC/ TC 65 in general handle Industrial communication networks – Network and system security in the context of Industrial Automation and Control Systems (IACS).
Different subjects like Management System, Industrial IT Security, IACS and Embedded Security, Component are considered.
In the field of machinery safety and especially of functional safety IEC/ TC 44 is responsible and has the expertise. Security may have an negative influence on functional safety and guidance are necessary in a such complex environment.
IEC/ TC 44 decided in the last plenary meeting to consider the security aspects in context of safety of machinery.

Therefore the following aspects have to be considered:
– what is the relationship between safety and security;
– vulnerabilities can be the result of systematic fault which can lead to a hazardous situation of the machine;
– vulnerabilities may impact the integrity and availability of the safety-related control system to properly perform its function(s);
– reasonable foreseeable misuse (see ISO 12100), e.g. typical use case definition and application of a corresponding threat model.

Target date	for first CD July 2017	for IS/ TS December 2019
Estimated number of meetings 8	Frequency of meetings: 3 per year	Date and place of first meeting: September 2016
Proposed working methods	☒ E-mail	☒ Collaboration tools

Relevant documents to be considered

IEC 61508, IEC 62443, IEC 61511, IEC 62061, ISO 13849-1, ISO 12100

[1] Other TC/SCs are requested to indicate their interest, if any, in this NP to the TC/SC secretary.

Copyright © 2016 International Electrotechnical Commission, IEC. All rights reserved. It is permitted to download this electronic file, to make a copy and to print out the content for the sole purpose of preparing National Committee positions. You may not copy or "mirror" the file or printed version of the document, or any part of it, for any other purpose without permission in writing from IEC.

® Registered trademark of the International Electrotechnical Commission

Relationship of project to activities of other international bodies

IEC 62443series (IEC/ TC 65), IEC 62061 (IEC/ TC 44 WG 7), ISO 13849-1 (ISO/ TC 199 WG 8), ISO 12100 (ISO/ TC 199 WG5)

Liaison organizations	**Need for coordination within ISO or IEC** IEC/ TC 65, ISO/ TC 199

Preparatory work

Ensure that all copyright issues are identified. Check one of the two following boxes

☒ A draft is attached for comment* □ An outline is attached

* Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

We nominate a project leader as follows in accordance with ISO/IEC Directives, Part 1, 2.3.4 (name, address, fax and e-mail):

Patrick Gehlen
Siemens AG
Schuhstr. 60, 91052 Erlangen (Germany)
Phone: +49 173 707 32 74
email: patrick.gehlen@siemens.com

® Registered trademark of the International Electrotechnical Commission

Concerns known patented items (see ISO/IEC Directives, Part 2) □ Yes. If yes, provide full information as an annex ☒ no	**Name and/or signature of the proposer** German National Committee of IEC/ TC 44

Comments and recommendations from the TC/SC officers

1) Work allocation

□ Project team ☒ New working group □ Existing working group no:

2) Draft suitable for direct submission as

☒ CD □ CDV/ DTS

3) General quality of the draft (conformity to ISO/IEC Directives, Part 2)

□ Little redrafting needed ☒ Substantial redrafting needed □ no draft (outline only)

4) Relationship with other activities

In IEC
IEC 62061 (IEC/ TC 44 WG 7), IEC 62443series (IEC/ TC 65)

In other organizations
ISO 13849-1 (ISO/ TC 199 WG 8),ISO 12100 (ISO/ TC 199 WG 5)

5) Proposed horizontal standard

□ [1]

Remarks from the TC/SC officers

[1] Other TC/SCs are requested to indicate their interest, if any, in this NP to the TC/SC secretary.

Approval criteria:

- Approval of the work item by a simple majority of the P-members voting;
- At least 4 P-members in the case of a committee with 16 or fewer P-members, or at least 5 P-members in the case of committees with more than 17 P-members, have nominated or confirmed the name of an expert and approved the new work item proposal.

Elements to be clarified when proposing a new work item

Title

Indicate the subject matter of the proposed new standard or technical specification.

Indicate whether it is intended to prepare a standardor a technical specification.

Scope

Give a clear indication of the coverage of the proposed new work item and, if necessary for clarity, exclusions.

Indicate whether the subject proposed relates to one or more of the fields of safety, EMC, the environment or quality assurance.

Purpose and justification

Give details based on a critical study of the following elements wherever practicable.

a) The specific aims and reason for the standardization activity, with particular emphasis on the aspects of standardization to be covered, the problems it is expected to solve or the difficulties it is intended to overcome.

b) The main interests that might benefit from or be affected by the activity, such as industry, consumers, trade, governments, distributors.

c) Feasibility of the activity: Are there factors that could hinder the successful establishment or general application of the standard?

d) Timeliness of the standard to be produced: Is the technology reasonably stabilized? If not, how much time is likely to be available before advances in technology may render the proposed standard outdated? Is the proposed standard required as a basis for the future development of the technology in question?

e) Urgency of the activity, considering the needs of the market (industry, consumers, trade, governments etc.) as well as other fields or organizations. Indicate target date and, when a series of standards is proposed, suggest priorities.

f) The benefits to be gained by the implementation of the proposed standard; alternatively, the loss or disadvantage(s) if no standard is established within a reasonable time. Data such as product volume of value of trade should be included and quantified.

g) If the standardization activity is, or is likely to be, the subject of regulations or to require the harmonization of existing regulations, this should be indicated.

If a series of new work items is proposed, the purpose and justification of which is common, a common proposal may be drafted including all elements to be clarified and enumerating the titles and scopes of each individual item.

Relevant documents

List any known relevant documents (such as standards and regulations), regardless of their source. When the proposer considers that an existing well-established document may be acceptable as a standard (with or without amendments), indicate this with appropriate justification and attach a copy to the proposal.

Cooperation and liaison

List relevant organizations or bodies with which cooperation and liaison should exist.

Preparatory work

Indicate the name of the project leader nominated by the proposer.

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

New work item Proposal - Draft for Committee

Remarks:

- **((editor note: ...))** to be discussed in the future working group

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.

International Standard IEC XXXXX has been prepared by IEC technical committee 44: Safety of machinery – Electrotechnical aspects.

The text of this standard is based on the following documents:

FDIS	Report on voting
XX/XX/FDIS	XX/XX/RVD

Full information on the voting for the approval of this standard 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.

The National Committees are requested to note that for this publication the stability date is 20XX.

THIS TEXT IS INCLUDED FOR THE INFORMATION OF THE NATIONAL COMMITTEES AND WILL BE DELETED AT THE PUBLICATION STAGE.

INTRODUCTION

More and more industrial systems are under attack due to the fact that:

- internal foreseeable misuse, e.g. change management for re-programming of safety functions of a machine, access control for key-interlocks, access to dedicated operating safety functions, …
- “convergence” between standard IT and industrial systems is increasing;
- operating systems like Linux 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 or open source software components (COTS 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;

In general safety systems are subject to the current security threats. Due to the nature of the safety systems, where a security incident e.g. can lead to a malfunction of the safety function or the intentional activation of the safety function, security threats must be considered, in order to reduce e.g. the likelihood of sabotage and for damaging reputation.

The risk potential of attack opportunities is significant seeing the trends and developments of threats and the amount of known vulnerabilities.

Therefore 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, SIL acc. to IEC 62061 or PL acc. to ISO 13849-1.

With respect to the safety function the security threads (internal or external) might impact the safety integrity and the overall system availability.

NOTE 1 In order to ensure the security objectives the standard IEC 62443-3-3 defines and recommends security requirements (“foundational requirements”) to be fulfilled by the relevant system.

NOTE 2 The assumed “hierarchy model” and “zones and conduits model” of IEC 62443-3-2 do not necessarily reflect the machinery sector.

SAFETY OF MACHINERY–

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

1 Scope

This International Standard / This part of IEC 6XXXX considers only those aspects of security threats and vulnerabilities that relate to the functional safety of machinery control systems and which may lead to the loss of the ability to maintain safe operation of a machine (safety measures).

NOTE 1 For other aspects of security threats and vulnerabilities the provisions of the IEC 62443 series can apply.

NOTE 2 This guidance could also be used by other Technical Committees and for non-safety-related control system.

Aspects to be considered are:

- what is the relationship between safety and security;
- vulnerabilities can be the result of systematic fault which can lead to a hazardous situation of the machine;
- vulnerabilities may impact the integrity and availability of the safety-related control system to properly perform its function(s);
- reasonable foreseeable misuse (see ISO 12100), e.g. typical use case definition and application of a corresponding threat model.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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*

ISO 13849-2:2015, *Safety of machinery – Safety-related parts of control systems – Part 2: Validation*

IEC 60204–1, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

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

3 Terms and definitions

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

For the purposes of this document, the terms and definitions given in [*another publication*] and the following apply.

3.1.1
asset

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

[SOURCE: IEC 62443-3-3, 3.1.1 modified]

3.1.2
attack

assault on a system that derives from an intelligent threat

[SOURCE: IEC 62443-3-3, 3.1.3]

3.1.3
availability
property of ensuring timely and reliable access to and use of control system information and functionality

[SOURCE: IEC 62443-3-3, 3.1.8]

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

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

Note to entry 3 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, 3.2.16]

3.1.4
confidentiality

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

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

3.1.5
(machine) 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 EUC is put into a hazardous or potentially hazardous state; or

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

[SOURCE: IEC 61508-4, 3.6.7]

3.1.7
risk

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

[SOURCE: ISO 12100, 3.12]

3.1.8
safety
freedom from unacceptable risk

[SOURCE: ISO/IEC Guide 51:1999, definition 3.1]

3.1.9
safety function

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

[SOURCE: ISO 12100, 3.30]

3.1.10
safety integrity

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

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

Note to entry 2 There are four levels of safety integrity (see 3.5.8).

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

Note to entry 4 Safety integrity comprises hardware safety integrity (see 3.5.7) and systematic safety integrity (see 3.5.6).

Note to entry 5 This definition focuses on the reliability of the safety-related systems to perform the safety functions (see IEV 191-12-01 for a definition of reliability).

[SOURCE: IEC 61508-4, 3.5.4]

3.1.11
SCS
Safety-related Control System
electrical control system of a machine whose failure can result in an immediate increase of the risk(s)

Note 1 to entry: A SCS includes all parts of an electrical control system whose failure may result in a reduction or loss of functional safety and this can comprise both electrical power circuits and control circuits.

Note 2 to entry: Is equivalent to SRECS of IEC 62061 or one or several SRP/CS of ISO 13849-1.

3.1.12
security
(1) measures taken to protect a system

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

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

(4) 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

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

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

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

information security

preservation of confidentiality (2.12), integrity (2.40) and availability (2.9) of information

Note 1 to entry: In addition, other properties, such as authenticity (2.8), accountability, non-repudiation (2.54), and reliability (2.62) can also be involved.

[SOURCE: ISO/IEC 27000:2014, 2.33]

3.1.13
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, 3.2.87]

3.1.14
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, 3.4.4, modified]

3.1.15
threat

(1) 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, 3.1.44]

(2) potential cause of an unwanted incident, which may result in harm to a system or organization

[SOURCE: ISO/IEC 27000:2014, 2.83]

3.1.16
vulnerabilities

(1) inherent weaknesses in systems, components, or organizations that could be exploited or triggered by a threat source.

NOTE Vulnerabilities may be the result of intentional design choices or may be accidental, resulting from the failure to understand the operational environment. They may also emerge as equipment ages and eventually becomes obsolete, which occurs in a shorter time than is typical for the underlying process or equipment under control. Vulnerabilities are not limited to the electronic or network systems. Understanding the interaction between physical (including human) and electronic vulnerabilities is critical to establishing effective industrial automation and control system security.
An industrial automation and control system that initially has limited vulnerability may become more vulnerable with situations such as changing environment, changing technology, system component failure, unavailability of component replacements, personnel turnover, and greater threat intelligence.

[SOURCE: IEC/TS 62443-1-1, 5.6.3, modified]

(2) weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

[SOURCE: NIST Special Publication 800-82, Revision 2 Initial Public Draft]

(3) weakness of an asset or control (2.16) that can be exploited by one or more threats (2.83)

[SOURCE: ISO/IEC 27000:2014, 2.89]

(4) A flaw or weakness in a system’s design, implementation, or operation and management that could be exploited to violate the system’s integrity or security policy.

[SOURCE: RFC 2828]

4 Safety and security objectives

4.1 General

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

– a machine shall have appropriate safety measures, regardless of security vulnerabilities;

– each safety measure can have security measures (e.g. authentication, authorization, data integrity) to prevent unauthorized manipulation (reasonably foreseeable misuse) of the safety measure;

– security measure(s) shall be appropriate to maintain the performance of safety function(s).

4.2 Safety objectives

Safety of machinery is basically defined by the (safety) risk assessment and the derived risk reduction measures.

The strategy for risk reduction at the machine is given in ISO 12100 and is described by the term “risk assessment”.

NOTE 1 The risk assessment including the implemented risk reduction measures will be applied by the designers during the development of machinery to enable the design of machines that are safe for their intended use.

From the risk reduction strategy, as outlined in ISO 12100, any need for safety functions will be determined. Safety function(s) that are performed by a safety-related control system (SCS) need to achieve a safety integrity (performance) as SIL acc. to IEC 62061 or PL acc. to ISO 13849-1, depending on the risk estimation.

NOTE 2 Functional safety (safety measure) is based on

- *Integrity* (e.g. against random errors or against deterministic errors) of safety-related control system performing safety function(s)
- *Availability* of the safety function (this includes the transition into a safe but non-productive state where the availability of the operation function is not guaranteed)

4.3 Security objectives

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

NOTE Examples of security objectives are:

- *Integrity* against manipulations;
- *Confidentiality* by means of encryption;
- *Availability* (usually and very generally) of secured function.

Security risks will be evaluated by using a security risk assessment in order to identify the security objectives and to derive security (counter) measure(s).

4.3.1 Security risk assessment

In general a security risk assessment is based on a product / system security context on which threats and known vulnerabilities are applied. The aim of this activity is to define relevant (counter) measures to fulfil the overall security objectives.

NOTE 1 Based on IEC/TS 62443-1-1, 5.5 and Figure 4.

In the context of safety of machinery the overall security objective is to protect the ability to maintain safe operation of a machine (safety measures) related to safety-related control systems. Therefore all relevant threats and known product / system vulnerabilities possibly effecting the safe operation shall be considered (see Figure 1) and documented as part of the security risk assessment.

Due to the nature of threats and known vulnerabilities the security risk assessment shall be carried out periodically.

NOTE 2 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 a safety-related control system.

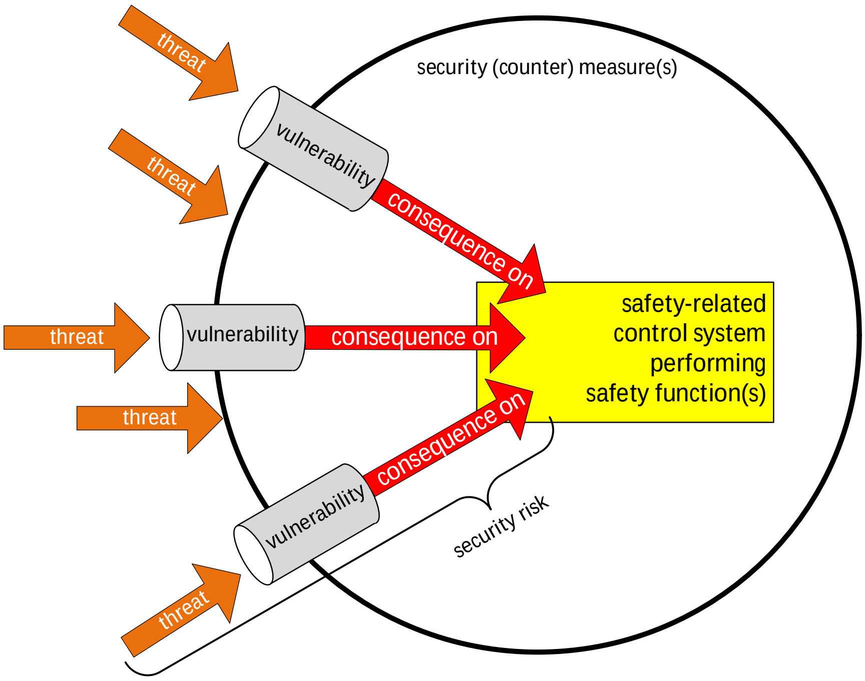

Figure 1 – Relationship between threat(s), vulnerabilities, consequence(s) and security risk(s) for safety-related control system(s) performing safety function(s)

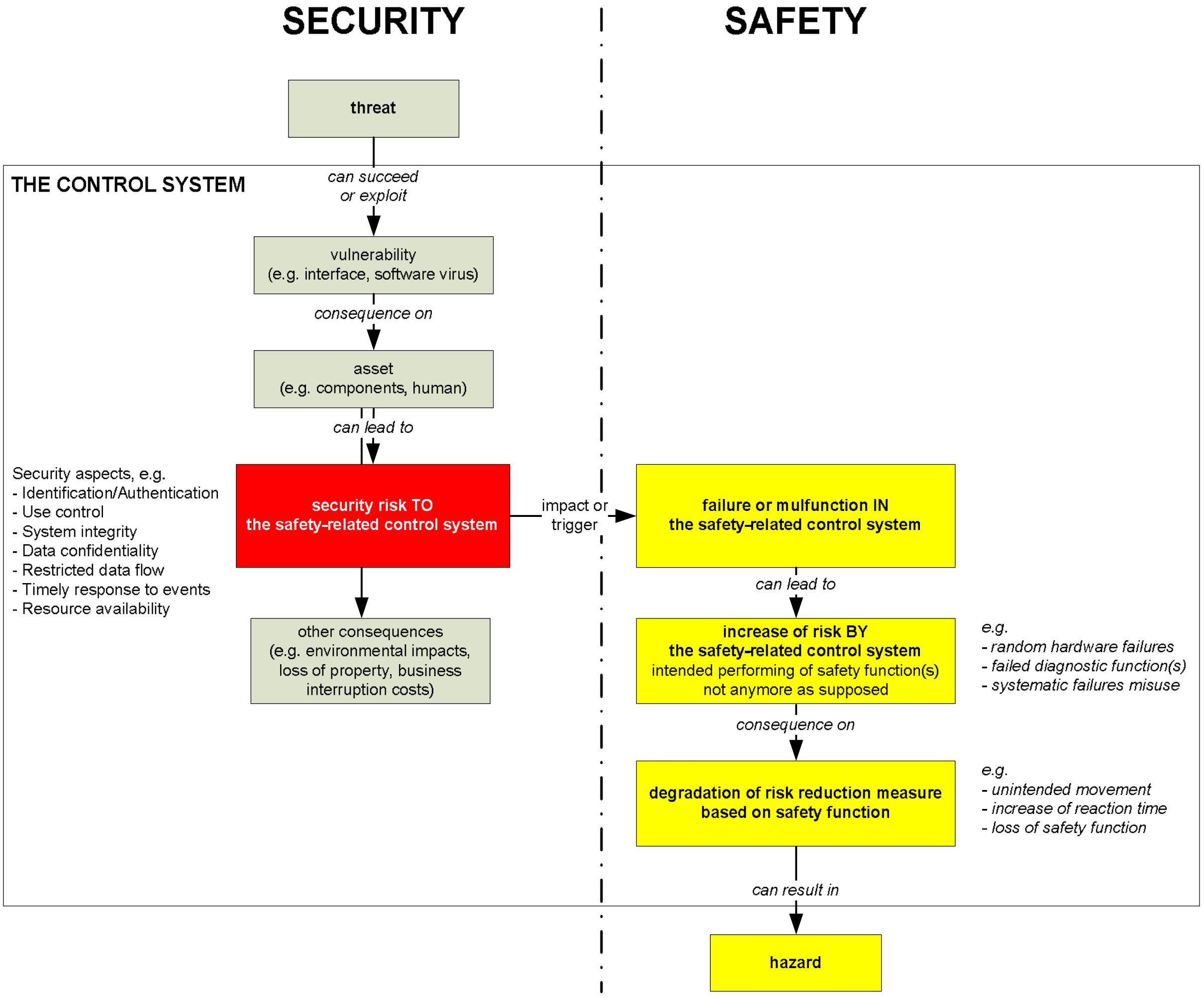
SECURITY
SAFETY
threat
THE CONTROL SYSTEM
can succeed or exploit
vulnerability (e.g. interface, software virus)
consequence on
asset (e.g. components, human)
can lead to
Security aspects, e.g.
- Identification/Authentication
- Use control
- System integrity
- Data confidentiality
- Restricted data flow
- Timely response to events
- Resource availability
security risk TO the safety-related control system
impact or trigger
failure or mulfunction IN the safety-related control system
other consequences (e.g. environmental impacts, loss of property, business interruption costs)
can lead to
increase of risk BY the safety-related control system intended performing of safety function(s) not anymore as supposed
e.g.
- random hardware failures
- failed diagnostic function(s)
- systematic failures misuse
consequence on
degradation of risk reduction measure based on safety function
e.g.
- unintended movement
- increase of reaction time
- loss of safety function
can result in
hazard

Figure 2 – Possible effects of security risk(s) to a safety-related control system

4.3.2 Security (counter) measures

The results of the security risk assessment are the input for the security requirements specification which defines the security (counter) measures.

Those security (counter) measures shall take into account appropriately the required safety integrity of the safety-related control system (SCS) performing the safety function(s) (see Figure 3).

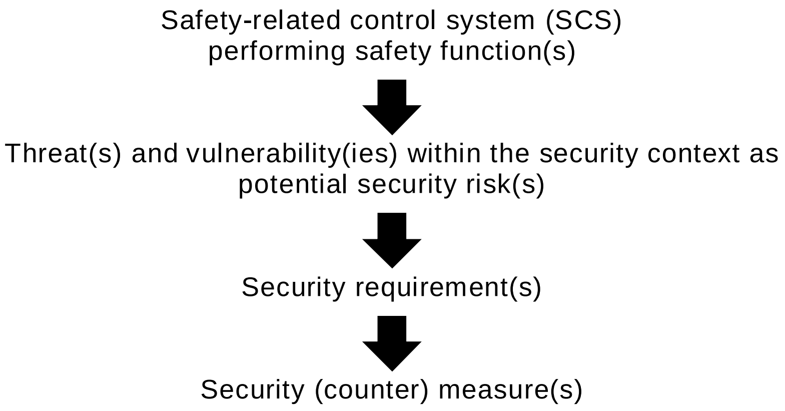
Safety-related control system (SCS) performing safety function(s)
Threat(s) and vulnerability(ies) within the security context as potential security risk(s)
Security requirement(s)
Security (counter) measure(s)

Figure 3 – Workflow determining security (counter) measure(s) based on safety-related control system(s) performing safety function(s)

NOTE Security (counter) measures basically are systematic measures and can have also an impact on safety measure(s).

5 Security requirements related to functional safety

5.1 General

((editor note: IEC/FDIS 61511-1:2015, 8.2.4, modified))

The security risk assessment shall be carried out at each lifecycle phase by the designer of the machinery and the end user of machinery.

NOTE 1 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);
- 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 security risk assessment shall be carried out to identify the threats and vulnerabilities of the safety-related control system within a defined security context. It shall result in:

a) a description of the devices covered by a security risk 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 (including intentional attacks on the hardware, application programs and related software, as well as unintended events resulting from human error);

NOTE 2 Vulnerabilities may be the result of intentional design choices or may be accidental, e.g. resulting from the failure to understand the operational environment.

c) a description of the potential consequences resulting from the security risks, by considering the possibility under which condition these can occur;

d) consideration of various phases such as design, implementation, commissioning, operation, and maintenance;

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

e) the determination of requirements for additional measures;

NOTE 4 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.

f) a description of, or references to information on the measures taken to reduce or remove the threats.

NOTE 5 A safety-related control system that initially has limited vulnerability may become more vulnerable with situations such as changing environment, changing technology, system component failure, unavailability of component replacements, personnel turnover, and greater threat intelligence.

5.2 Security risk mitigation

((editor note: IEC/TS 62443-1-1, 5.6.4.3; IEC/TR 62351-12, modified))

NOTE 1 The comparable term to “risk mitigation” is the term “risk reduction” used in safety of machinery.

There are several potential responses to security risks:

a) design the security risk out (avoid);

b) reduce the security risk (limit);

c) accept the security risk;

d) transfer or share the security risk (to a third entity);

The security risk mitigation strategy in the field of safety of machinery depends on the environment of the machine (e.g. location and organization).

The vulnerabilities of the safety-related control system performing safety function(s) of the machine will be the base or input for the final mitigation strategy.

Figure 4 shows in this context the interrelationship between the designer of the safety-related control system (manufacturer of machine(s)) and the user of the safety-related control system (user of machine(s)).

NOTE 2 Example: Consideration of a safety system with error correcting code for memory done by hardware. Attackers are looking for a place to store their malware and place it in the safety system, by just adding their code to firmware and adjusting the firmware’s signature (because the algorithm was patented by the manufacturer). Because the malware does not follow any coding standards, it keeps storing its temporary results in the same memory area as the safe functions do. Error correcting code in hardware ensures the integrity of the (wrong) data. Safety functions now work with different data (thresholds for monitoring functions, results of checks etc.), which obviously changes the integrity of the safety system, and hence the level of risk reduction. Also, safety related reliability analyses are not valid any more, since assumptions on base failure rate of memory and diagnostic coverage of error correcting code are not valid any more. Note that the attackers did not, at any point, intend to change the safety functions. The vulnerability was publishing the algorithm for the firmware signature, which was intended to protect against random failures in the first place.

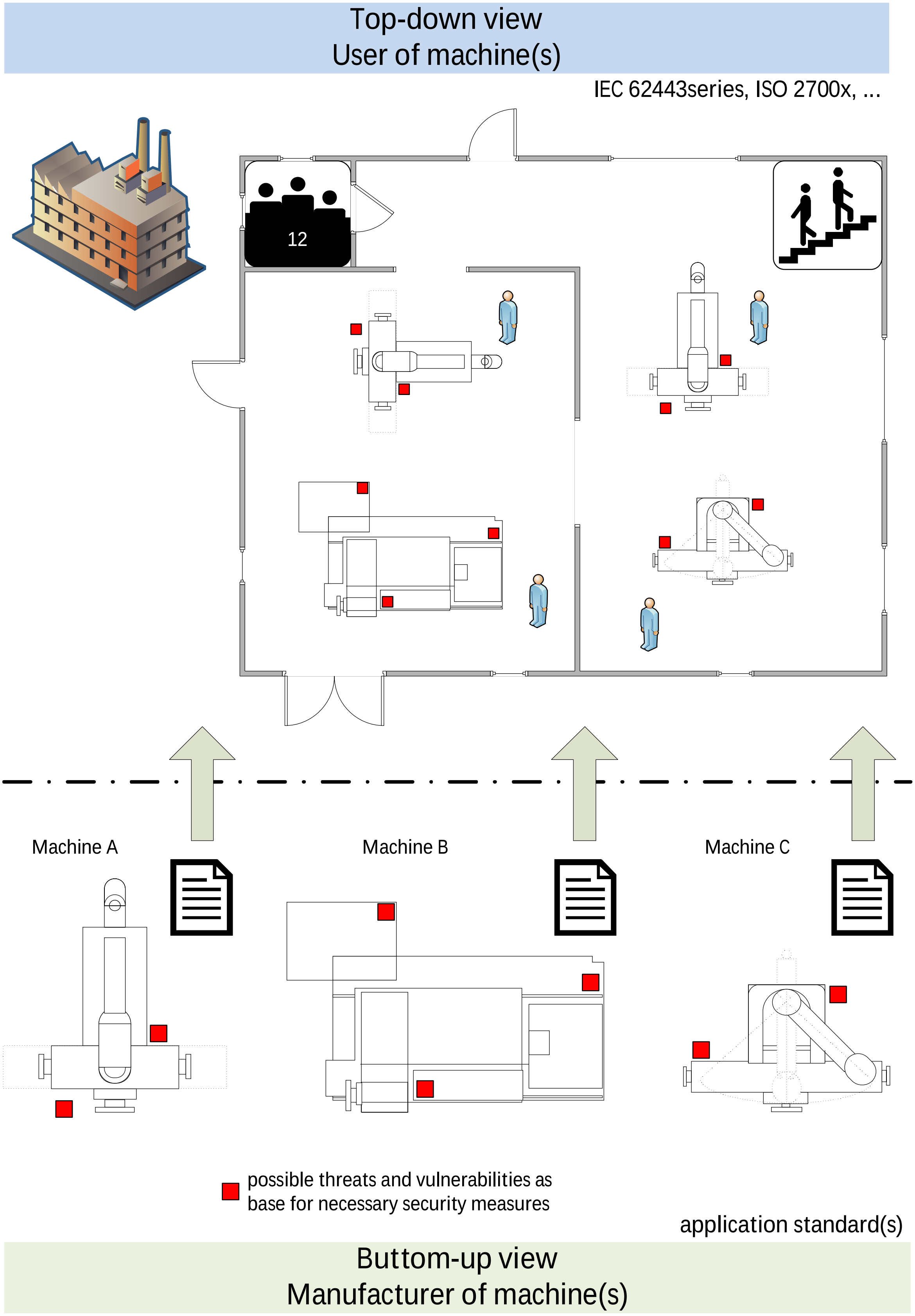
Top-down view
User of machine(s)
IEC 62443series, ISO 2700x, ...
12
Machine A
Machine B
Machine C
🟥 possible threats and vulnerabilities as base for necessary security measures
application standard(s)
Buttom-up view
Manufacturer of machine(s)

Figure 4 – Interrelationship between manufacturer of machine(s) (designer) and user of machine(s)

5.3 Security Requirements Specification

Based on the vulnerabilities (defined by the threat-risk assessment) of the safety-related control system a security requirements specification shall be generated.

Following information at least shall be available:

– the safety-related control system performing the safety function(s);

– potential source of security lack (threats, vulnerabilities) based on the safety-related control system;

– description of safety function(s);

– consequences on the safety function(s);

– description of proposed security (counter) measure(s).

5.4 Security (counter) measures

Any security (counter) measure shall not influence the safety-related control system, e.g.:

– deeper investigation of mutual influences of safety and security (counter) measures (e.g. response time of safety function);

– conceptual inclusion of product safety (attacks may not effect functional safety of the plant but safety-related characteristics of the product, e.g. food and drugs);

– analysis of other approaches to safety where safety-related and normal operation function (machine functions) are merged (e.g. medical devices).

Verification of security (counter) measures shall be done periodically during normal operation of machinery by reassessing threat-risks.

Especially the following topics should be considered:

– network architecture;

NOTE Examples for architectural issues relevant to the safety-related control system can be:

a) network design;

b) firewall configuration;

c) user authorization and authentication;

d) interconnecting different process control networks;

e) wireless communications;

h) access to external networks (i.e., the internet).

– portable devices;

– wireless devices and sensors (this is part of the previous network architecture);

– remote access.

The following basic requirements allow evaluating security (counter) measures related to safety-related control system(s).

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

Table 1 — Possible assignment of basic requirements of security to impact(s) on a safety-related control system

Security basic requirements	Description	**Safety of Machinery** possible impact(s) on a safety-related control system
Identification and authentication	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 IACS and monitor the use of these privileges.	Modification or manipulation
System integrity	Ensure the integrity of the control system to prevent unauthorized manipulation.	Impact on safety integrity
Data confidentiality	Ensure the confidentiality of information on communication channels and in data repositories to prevent unauthorized disclosure	Not relevant for safety integrity
Restricted data flow	Segment the control system via zones and conduits to limit the unnecessary flow of data.	**((editor note: to be considered if relevant))**
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.	**((editor note: to be considered if relevant))**
Resource availability	Ensure the availability of the control system against the degradation or denial of essential services.	Safety integrity

NOTE Based on foundational requirements of IEC/TS 62443-1-1, 5.3 and IEC 62443-3-3, Annex B.

5.4.1 Identification and authentication

Where interfaces of the safety-related control system provide human user access to this safety-related control system, the capability to identify and authenticate all human users shall be considered.

Examples to preventing e.g. unauthorized access and modification are:

- human user identification and authentication;
- authentication for networks;
- software account management;
- wireless access management;
- strength of password-based authentication;
- password generation and lifetime restrictions for human users.

5.4.2 Use Control

When a user is identified and authenticated, it can be necessary that the safety-related control system has to restrict the allowed actions to the authorized use of the safety-related control system (assigned privileges of an authenticated user).

The safety-related control system shall support a dual approval where an action can result in serious impact on the safety-related control system.

NOTE For example the change of safety-related data for speed monitoring.

For example the following topics can be relevant:

- Use control for portable and mobile devices;
- Remote session termination;
- Response to audit processing failures.

5.4.3 System integrity

The user of the machine(s) (asset owner) is responsible for maintaining the system integrity of the safety-related control system implemented by the (original) designer (normally manufacture of the machine(s)).

To maintain the safety integrity level of the safety-related control system the following aspects can be relevant:

- communication integrity/corruption (LAN, WLAN, ...), e.g. using of cryptographic integrity protection (e.g. VPN);
- malicious code protection (against manipulation, for example, viruses, worms, Trojan horses and spyware), e.g. consideration of concerned interfaces (e.g. USB, programming interface for PLC, ...);
- software and information integrity (unauthorized changes);
- input validation (rules for checking the input data, out-of-range values);
- deterministic safe state as result of threat actions.

5.4.4 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 data-stores require protection against eavesdropping and unauthorized access.

In context of control system(s) this aspect may be relevant, but it is not within the scope of this document.

5.4.5 Restricted data flow

((editor note: to be considered if relevant))

The user of the machine(s) (asset owner) needs to determine necessary information flow restrictions and thus, by extension, determine the configuration of the conduits used to deliver this information.

This aspect is to be considered in the overall security risk assessment and can be relevant in context of control system(s).

Following topic can be relevant e.g. to ensure the reaction time of the safety-related control system:

- Network segmentation.

5.4.6 Timely response to events

((editor note: to be considered if relevant))

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

This aspect is to be considered in the overall security risk assessment and not specific to safety-related control systems.

5.4.7 Resource availability

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

This aspect is to be considered in the overall security risk assessment and can be relevant in context of control system(s).

Following topic can be relevant e.g. to ensure the performance of the safety-related control system:

- resource management (for example, network segmentation or priority schemes);

– network and security configuration settings.

6 Validation of security measures

((editor note: to be discussed if helpful; parts of IEC 62443-4-1 to be included?))

7 Documentation

((editor note: IEC 62443-4-1, Practice 8 Security Guidelines to be included?))

The designer of the safety-related control system shall provide documentation to the user of the safety-related control system in order to provide a list of any relevant security risks and the proposed risk mitigation measures (categories) to be considered.

The following security risk aspects as security vulnerabilities shall be mentioned:

– devices covered by the security risk assessment;

– considered phases (design, implementation, commissioning, operation, and maintenance);

– measures against unauthorized access and modification, if relevant;

– measures to ensure system integrity, especially by considering interfaces, software, and communication, if relevant.

Table 2 shows an example how to document the results based on the security risk analysis.

Table 2 — Example of documentation of security (counter) measures

Designer of SCS performing safety function(s) for safety of machinery				User of machinery
Source of security lack (threats, vulnerabilities)	**Safety function, (impacted SCS)**	**Potential Consequences**	**Description of proposed security measure(s)**	**Implemented security measure(s)**
Unauthorized access (identification) and use control				

Designer of SCS performing safety function(s) for safety of machinery				User of machinery
Source of security lack (threats, vulnerabilities)	**Safety function, (impacted SCS)**	**Potential Consequences**	**Description of proposed security measure(s)**	**Implemented security measure(s)**
System integrity (interfaces, software, communication)				

Annex A
(informative)

Basic information related to threats and threat modelling approach

((editor note: IEC/TS 62443-1-1; IEC 62443-4-1, SR-2 Threat model to be considered?))

A.1 Evaluation of threats

Threats describe 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
  a) **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.”
  b) **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:
  c) <u>Communication</u>: The intent of a communication attack is to disrupt communications for control systems;
  d) <u>Database injection</u>: Injection attacks are used to steal information from a database;
  e) <u>Replay</u>: 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;
  f) <u>Spoofing and impersonation</u>: In networking, the term is used to describe a variety of ways in which hardware and software can be fooled;
  g) <u>Social engineering</u>: Threat agents also obtain or attempt to obtain otherwise secure data by tricking an individual into revealing secure information;

h) Phishing: Phishing relies on social engineering in that humans tend to believe in the security of a brand name, associating it with trustworthiness;

i) Malicious code: Malicious code attacks can take the form of viruses, worms, automated exploits, or Trojan Horses;

j) Denial of service (DoS): Denial (or degradation) of service attacks affect the availability of a network, operating system, or application resources;

k) Escalation of privileges: With these increased privileges the attacker can take actions that would otherwise be prevented;

l) 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 See also IEC/TS 62443-1-1, 5.6.5 for further information.

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

There should be a definition and evaluation of threats that can impact the safety function(s) performed by a safety-related control system (SCS), using one or several safety-related devices.

Consideration should be given to the possible access to the devices comprising of the safety-related control system by any person with malicious intent. 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, e.g.

1) an interactive screen or control panel,

2) switches or buttons for device configuration or

3) 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.

It may be possible that an attack can occur indirectly to the safety-related device, for example by:

4) computer technology,

5) network communication technology or

6) wireless communication technology

In these tree 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 (counter) measures must 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.

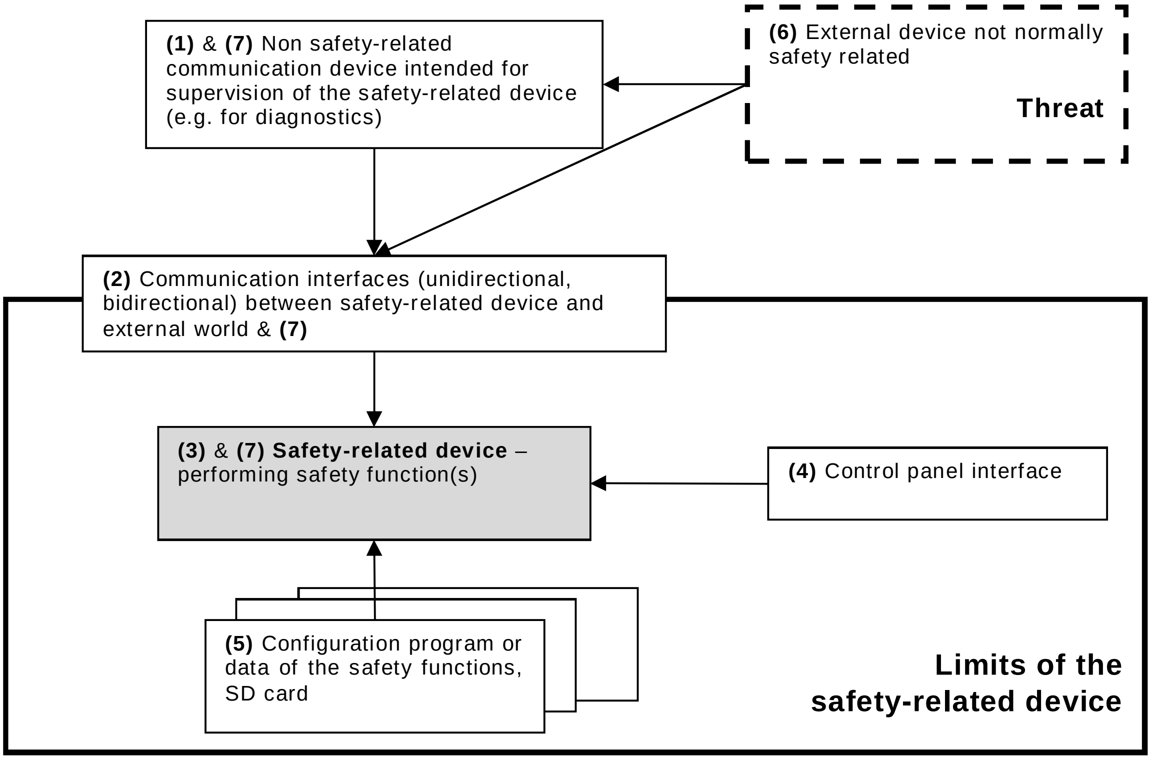
(1) & (7) Non safety-related communication device intended for supervision of the safety-related device (e.g. for diagnostics)
(6) External device not normally safety related
Threat
(2) Communication interfaces (unidirectional, bidirectional) between safety-related device and external world & (7)
(3) & (7) Safety-related device – performing safety function(s)
(4) Control panel interface
(5) Configuration program or data of the safety functions, SD card
Limits of the safety-related device

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

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

Level	Comments
(1)	The communication from a supervisionary device to the safety-related device can be open to an attack on the safety-related device and a failure of or threat to this supervision 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 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 counter measures 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 describes 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.

A.3 Security risk mitigation for a safety-related control system as part of overall security risk mitigation process

To implement risk assessment and risk reduction the designer should implement the following process in the order given (see also Figure A.2):

a) Determination of the SL-T (Target Security Level) for the machinery control system. This shall include intended use and any reasonably foreseeable misuse. Where possible there should be discussion with the end user of the machinery;

   NOTE 1 For more information see A.2.2 Types of SLs in IEC 62443-3-3.

b) Identification of hazards and associated hazardous situations to define the required safety functions (see ISO 12100, IEC 62061, ISO 13849);

c) Evaluation of security risk(s) to the safety function(s) and decisions about the need for security risk mitigation (reduction). The following hierarchy should be used. This is similar to the risk reduction process as for safety of machinery according to ISO 12100):

   – inherently secure,

   – use of safety measure against security threat,

   – use of security (counter) measures;

d) Implementation of security (counter) measures related to threats not leading to modification or alteration of the related safety function(s) performed by a safety-related control system.

It may be necessary for this process to be iterative in order to eliminate hazards, threats and vulnerabilities as far as practicable and to reduce adequately risks by the implementation of protective measures.

NOTE 2 It is assumed that hazards or threats and vulnerabilities will sooner or later lead to harm if no protective measure or security (counter) measures have been implemented.

Protective measures are the combination of any security (counter) measures and safety function(s) implemented by the designer and the user in accordance with Figure A.2. Security (counter) measures and updates which are designed by the manufacturer are preferable to those implemented by the user and usually prove more effective.

The objective is to achieve the greatest practicable risk reduction, taking into account the five aspects below:

- the safety of machinery during all life cycle phases;
- the ability of the machine to perform its function;
- the security for the machinery during different phases of the security lifecycle;
- the usability of the machine;
- the manufacturing, operational and dismantling costs of the machine.

The strategy defined in this clause is represented by the flowchart in Figure A.2.

NOTE 3 The process itself can be iterative and several successive applications can be necessary to reduce the risk, making the best use of available technology.

NOTE 4 The ideal application of these principles requires knowledge of the intended and actual use of the machine, the accident history and health records, available risk reduction techniques, and the legal framework in which the machine is to be used.

NOTE 5 A machine design which is acceptable in terms of security risk mitigation (reduction) at a particular time could be no longer acceptable if the nature of the threat(s) changes.

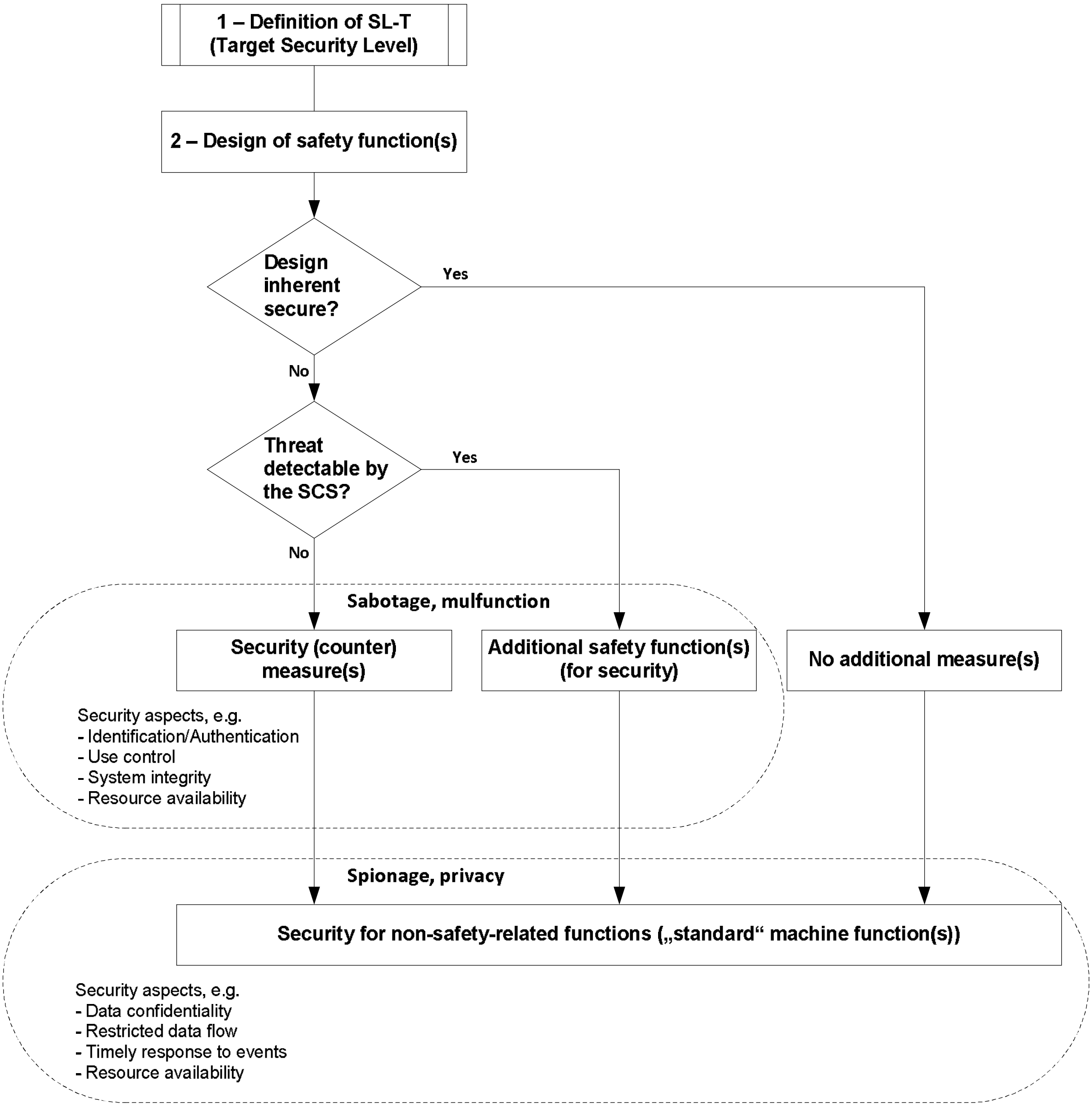
1 – Definition of SL-T (Target Security Level)
2 – Design of safety function(s)
Design inherent secure?
Yes
No
Threat detectable by the SCS?
Yes
No
Sabotage, mulfunction
Security (counter) measure(s)
Additional safety function(s) (for security)
No additional measure(s)
Security aspects, e.g.
- Identification/Authentication
- Use control
- System integrity
- Resource availability
Spionage, privacy
Security for non-safety-related functions („standard“ machine function(s))
Security aspects, e.g.
- Data confidentiality
- Restricted data flow
- Timely response to events
- Resource availability

Figure A.2 – Security risk mitigation process for a safety-related control system

Bibliography

IEC 61508-2, *Functional safety of electrical/electronic/ programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

IEC/TS 62443-1-1:2009, *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*

IEC 62442-2-1:2010, *Industrial communication Networks - Network and system security Part 2-1: Establishing an Industrial automation and control system security program*

IEC 62443-3-3:2013, *Security for industrial automation and control systems - Network and system, Security 3-3: System security requirements and security assurance levels*

IEC 62443-2-4:2015, *Security for industrial process measurement and control – Network and system security, Part 2-4: Certification of IACS supplier security policies and practices*

IEC WD 62443-4-1:2016, *Security for industrial process measurement and control – Network and system security, Part 4-1: Secure product development lifecycle requirements.*

IEC TR 62351-12, *Resilience and Security Recommendations for Power Systems with Distributed Energy Resources (DER) Cyber-Physical Systems*

____