ISO/TC 199/WG 5 N 375

REPLACES: ISO/TC 199/WG 5 N 364

ISO/TC 199/WG 5
General principles for the design of machinery and risk assessment
E-mail of Secretary: christian.thom@din.de
Secretariat: DIN

ISO/NP TR 22100-4:2017-08 (E) -- New work item proposal as forwarded to TC 199 for balloting

Date of document	2017-08-09
Expected action	Comment
Due Date	2017-09-01

Background

Dear expert,

please find attached the official new work item proposal form we completed on the basis of our consideration in Helsinki as well as the associated NP document which corresponds to the revision of document N 364 in accordance with the comments resolution results from Helsinki.

The NP ballot will officially be launched on 10th August 2017 and last until 2nd November 2017.

As you will notice from the attached new draft document there are still some open issues to be resolved at our forthcoming Cork meeting:

1) The definitions moved from our former "parking lot" to Clause 3 need to be reviewed. For some terms listed definitions need to be written or taken over from other already existing sources, i.e. preferably existing International Standards. In this context, some homework was agreed by Dr. Steiger in connection with the comments resolution on GS 6 (see document N 374).

2) The comments resolution on GS 13 (-> minor correction to Figure 3 of the enclosure) and, in particular, to comment OG 1 still need to be implemented in the new document version.

3) After incorporating the CRM results in the previous document version and restructuring the whole document as proposed by Dr. Steiger some subclauses/text parts remained which have been copied in for the time being as "parking lots" at the end of the new Clause 10. These "parking lots" need to be reviewed/revised, moved to appropriate text positions (in Clause 10 ?) or deleted.

4) With regard to 10.2 and 10.3 possible further concrete means need to be checked based on the references cited there.

5) The bibliographic references need to be completed after finalization of Clause 3.

In order to allow all WG 5 experts to study concrete proposals from your side to resolve the items 1) to 4) above in due time before we meet in Cork we kindly ask you submit your comments/remarks/suggestions (preferably by using the STD commenting template available from LL-Folder 05)

by 1st September 2017 at the very latest

directly to the WG 5 Secretariat, att. to christian.thom@din.de

For your support we thank you in advance.

Yours sincerely,

Dr. Christian Thom

Secretary to ISO/TC 199/WG 5

Form 4: New Work Item Proposal

Circulation date: 2017-08-09 Closing date for voting: 2017-11-02	Reference number: ISO/NP TR 22100-4 (to be given by Central Secretariat) ISO/TC 199 **N 1411**
Proposer (e.g. ISO member body or A liaison organization) ISO/TC 199	
Secretariat DIN	

A proposal for a new work item within the scope of an existing committee shall be submitted to the secretariat of that committee with a copy to the Central Secretariat and, in the case of a subcommittee, a copy to the secretariat of the parent technical committee. Proposals not within the scope of an existing committee shall be submitted to the secretariat of the ISO Technical Management Board.

The proposer of a new work item may be a member body of ISO, the secretariat itself, another technical committee or subcommittee, an organization in liaison, the Technical Management Board or one of the advisory groups, or the Secretary-General.

The proposal will be circulated to the P-members of the technical committee or subcommittee for voting, and to the O-members for information.

☒ The proposer has considered the guidance given in the Annex C during the preparation of the NWIP.

Proposal (to be completed by the proposer)

Title of the proposed deliverable.

English title:

Safety of machinery -- Relationship with ISO 12100 -- Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects

French title:

(In the case of an amendment, revision or a new part of an existing document, show the reference number and current title)

Scope of the proposed deliverable.

Based on ISO 12100 this part of ISO/TR 22100 gives machine manufacturers a guidance on potential security aspects in relation to machinery safety when putting a machine into service the first time. It provides essential information to identify and address IT-security threats which could influence machinery safety. This part of ISO/TR 22100 gives guidance but does not provide detailed specifications on how to address IT-security aspects which could influence machinery safety. This part of ISO/TR 22100 does not address the bypass or defeat of protective/risk reduction measures through physical manipulation.

Purpose and justification of the proposal*

The primary purpose of this document is to address machinery safety aspects that might be affected by security issues related to the direct or remote access to, and manipulation of, a safety-related control system(s) by persons for intentional abuse (unintended uses). Intentional abuse falls outside the scope of ISO 12100 and the risk assessment process.
IT-security risks which may have an influence on machine safety are constantly evolving during the whole life cycle of a machine. The same applies for the appropriate/necessary counter-measures.

Within this context the influence of the machine manufacturer is basically concentrated on measures relevant at the life cycle stage "putting the machine into service the first time". This requires in particular to incorporate in the machine those machine parts/components, which can be targets for IT-security risks (hardware and software), with certain state of the art features which can be helpful to avoid/restrict those risks (threats) as well as a design of the entire machine according to state of the art principles regarding IT security.

Apart from those direct measures regarding originally installed hardware and software as well as appropriate design of the entire machine regarding IT security, the significant contribution by the machine manufacturer can be made by appropriate information on the vulnerability analysis in its instruction handbook to the customer/end user (and possibly to the system integrator).

This part of ISO/TR 22100 provides guidance to the machinery manufacturer in order to address IT security risks as related to machinery safety.

Consider the following: Is there a verified market need for the proposal? What problem does this standard solve? What value will the document bring to end-users? See Annex C of the ISO/IEC Directives part 1 for more information. See the following guidance on justification statements on ISO Connect: https://connect.iso.org/pages/viewpage.action?pageId=27590861

Preparatory work (at a minimum an outline should be included with the proposal)

☒ A draft is attached ☐ An outline is attached ☐ An existing document to serve as initial basis

The proposer or the proposer's organization is prepared to undertake the preparatory work required:

☒ Yes ☐ No

If a draft is attached to this proposal:

Please select from one of the following options (note that if no option is selected, the default will be the first option):

☐ Draft document will be registered as new project in the committee's work programme (stage 20.00)

☒ Draft document can be registered as a Working Draft (WD – stage 20.20)

☐ Draft document can be registered as a Committee Draft (CD – stage 30.00)

☐ Draft document can be registered as a Draft International Standard (DIS – stage 40.00)

If the attached document is copyrighted or includes copyrighted content:

☐ The proposer confirms that appropriate permissions have been granted in writing for ISO or IEC to use that copyrighted content.

Is this a Management Systems Standard (MSS)?

☐ Yes ☒ No

NOTE: if Yes, the NWIP along with the Justification study (see Annex SL of the Consolidated ISO Supplement) must be sent to the MSS Task Force secretariat (tmb@iso.org) for approval before the NWIP ballot can be launched.

Indication(s) of the preferred type to be produced under the proposal.

☐ International Standard ☐ Technical Specification

☐ Publicly Available Specification ☒ Technical Report

Proposed development track

☐ 18 months* ☐ 24 months ☐ 36 months ☐ 48 months

Note: Good project management is essential to meeting deadlines. A committee may be granted only one extension of up to 9 months for the total project duration (to be approved by the ISO/TMB).

*DIS ballot must be successfully completed within 13 months of the project's registration in order to be elligible for the direct publication process

Draft project plan (as discussed with committee leadership)

Proposed date for first meeting:

Dates for key milestones: DIS submission

Publication

Known patented items (see ISO/IEC Directives, Part 1 for important guidance)

☐ Yes ☒ No

If "Yes", provide full information as annex

Co-ordination of work: To the best of your knowledge, has this or a similar proposal been submitted to another standards development organization?

☒ Yes ☐ No

If “Yes”, please specify which one(s):

IEC/CD 63074

A statement from the proposer as to how the proposed work may relate to or impact on existing work, especially existing ISO and IEC deliverables.
The proposer should explain how the work differs from apparently similar work, or explain how duplication and conflict will be minimized.

Although several other activities exist related to cyber security, none focus explicitly on the machinery

A statement from the proposer as to how the proposed work may relate to or impact on existing work, especially existing ISO and IEC deliverables.
The proposer should explain how the work differs from apparently similar work, or explain how duplication and conflict will be minimized.

safety aspects in general related to the machinery manufacturer putting the machine into use the first time. Other projects address functional safety over the whole life cycle of the machine which incorporates as well requirements to the machine user.

A listing of relevant existing documents at the international, regional and national levels.

IEC/CD 63074, (Draft) IEC/PAS 63088, VDMA Industry 4.0 Security Guidelines, NIST Special Publication 800-82

Please fill out the relevant parts of the table below to identify relevant affected stakeholder categories and how they will each benefit from or be impacted by the proposed deliverable(s).

	Benefits/impacts	**Examples of organizations / companies to be contacted**
Industry and commerce large industry	Guidance on machinery safety and IT- security risks	Trade associations and individual companies
Industry and commerce SMEs	Guidance on machinery safety and IT- security risks	Trade associations and individual companies
Government	Providing explanation in relation to existing legal requirements for machinery safety	Local and regional governmental institutions, safety agencies
Consumers		
Labour	Improved understanding of machinery safety and IT security risks	Safety agencies
Academic and research bodies		
Standards application businesses		
Non-governmental organizations		
Other (please specify)		

Liaisons: A listing of relevant external international organizations or internal parties (other ISO and/or IEC committees) to be engaged as liaisons in the development of the deliverable(s). ISO/TC 184, IEC/TC 44	**Joint/parallel work:** **Possible joint/parallel work with:** □ IEC (please specify committee ID) □ CEN (please specify committee ID) □ Other (please specify)
A listing of relevant countries which are not already P-members of the committee. Note: The committee secretary shall distribute this NWIP to the countries listed above to see if they wish to participate in this work	
Proposed Project Leader (name and e-mail address) Dr. Gerhard Steiger gerhard.steiger@vdma.org	**Name of the Proposer** (include contact information) Dr. Christian Thom (on behalf of ISO/TC 199/WG 5) christian.thom@din.de
This proposal will be developed by: ☒ An existing Working Group: ISO/TC 199/WG 5 □ A new Working Group: (Note: establishment of a new WG must be approved by committee resolution) □ The TC/SC directly □ To be determined:	

Supplementary information relating to the proposal

□ This proposal relates to a new ISO document

☒ This proposal relates to the adoption as an active project of an item currently registered as a Preliminary Work Item

□ This proposal relates to the re-establishment of a cancelled project as an active project

Other:

Maintenance agencies and registration authorities

□ This proposal requires the service of a maintenance agency. If yes, please identify the potential candidate:

□ This proposal requires the service of a registration authority. If yes, please identify the potential candidate:

NOTE: Selection and appointment of the MA or RA is subject to the procedure outlined in the ISO/IEC Directives, Annex G and Annex H, and the RA policy in the ISO Supplement, Annex SN.

☒ Annex(es) are included with this proposal (give details)

ISO/NP TR 22100-4:2017-08 (E)

Additional information/question(s)

ISO/TC 199/WG 5 N 375

Date: 2017-08-09

ISO/NP TR 22100-4:2017(E)

ISO/TC 199/SC /WG 5

Secretariat: DIN

Safety of machinery — Relationship with ISO 12100 — Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects

Sécurité des machines — Relation avec l'ISO 12100 — Partie 4: Titre de la partie

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

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

Document type: Technical Report
Document subtype:
Document stage: **New Work Item Proposal**
Document language: E

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

The committee responsible for this document is ISO/TC 199, *Safety of machinery*.

ISO/TR 22100 consists of the following parts, under the general title *Safety of machinery — Relationship with ISO 12100*:

— *Part 1: How ISO 12100 relates to type-B and type-C standards*

— *Part 2: How ISO 12100 relates to ISO 13849-1*

— *Part 3: Implementation of ergonomic principles in safety standards*

— *Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects*

Introduction

Internet, digital services and technology are important enablers for smart manufacturing which is one part of internet of things (IoT), see ISO/IEC 20924. For the manufacturing environment, vertical networking and horizontal integration across the entire value network and convergence of design, ordering, delivery and manufacturing capabilities are the foundations. This will result in the transformation of conventional value chains and the emergence of new business models. Smart products based on smart manufacturing know many details of how they were made, their performance and how they are being used. The digital representation and the physical product are linked and the digital content depends on lifecycle phase. Implementing smart manufacturing will create an efficient and highly responsive package by leveraging existing manufacturing systems, as well as technological and economic potential. Smart manufacturing increases the vulnerabilities of machinery to IT security threats.

Smart manufacturing will lead to the emergence of dynamic, real‐time optimized, self‐organizing value chains. This will require an appropriate regulatory framework as well as standardized interfaces and harmonized business processes. Smart manufacturing is characterized by

a) increased product flexibility,

b) new intrinsic built‐in product properties,

c) flexible work organization,

d) changed scale (up to a lot size 1) and location of manufacturing.

Smart manufacturing will require further expansion of the description of the network infrastructure to enable privacy, self-configuration and ease of use. Therefore, there is a need for fast available, robust and secure communication networks.

The primary purpose of this document is to address machinery safety aspects that might be affected by security issues related to the direct or remote access to, and manipulation of, a safety-related control system(s) by persons for intentional abuse (unintended uses). Intentional abuse falls outside the scope of ISO 12100 and the risk assessment process.

Current technologies enable machinery suppliers to monitor and/or improve machine performance remotely by adjusting parameters without having to be on site at the machine. This ability provides considerable benefits as machinery can be kept operating without the downtime and associated costs of a field service person making a service call.

However, this same capability to adjust machine parameters to improve performance lends itself to the possibility for other persons with nefarious or criminal intent to make adjustments that can put workers and others at risk of harm. For example, speeds or forces could be adjusted to dangerous levels, temperatures could be lowered below a kill step level resulting in food contamination, or error codes or messages could be erased or falsified.

Cybersecurity for machinery is an adaptation of existing and more complex organizational cybersecurity models.

Safety of machinery — Relationship with ISO 12100 — Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects

1 Scope

Based on ISO 12100 this part of ISO/TR 22100 gives machine manufacturers a guidance on potential security aspects in relation to machinery safety when putting a machine into service the first time. It provides essential information to identify and address IT-security threats which could influence machinery safety.

This part of ISO/TR 22100 gives guidance but does not provide detailed specifications on how to address IT-security aspects which could influence machinery safety.

This part of ISO/TR 22100 does not address the bypass or defeat of protective/risk reduction measures through physical manipulation.

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.

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 12100 and the following 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
antivirus tool
software products and technology used to detect malicious code, prevent it from infecting a system, and remove malicious code that has infected the system

3.2
attack
an attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality

[SOURCE: CNSSI-4009]

3.3
authentication
verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system

[SOURCE: NIST SP 800-53]

3.4
authorization
right or a permission that is granted to a system entity to access a system resource

[SOURCE: RFC 4949]

3.5
confidentiality
preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

[SOURCE: NIST SP 800-53]

3.6
control system
system in which deliberate guidance or manipulation is used to achieve a prescribed value for a variable

Note 1 to entry: Control systems include SCADA, DCS, PLCs and other types of industrial measurement and control systems.

3.7
encryption
cryptographic transformation of data (called “plaintext”) into a form (called “ciphertext”) that conceals the data’s original meaning to prevent it from being known or used

Note 1 to entry: If the transformation is reversible, the corresponding reversal process is called “decryption,” which is a transformation that restores encrypted data to its original state.

[SOURCE: RFC 4949 – modified, original definition text divided in definition and Note to entry]

3.8
firewall
an inter-network gateway that restricts data communication traffic to and from one of the connected networks (the one said to be “inside” the firewall) and thus protects that network’s system resources against threats from the other network (the one that is said to be “outside” the firewall)

[SOURCE: RFC 4949]

an inter-network connection device that restricts data communication traffic between two connected networks.

Note 1 to entry: A firewall may be either an application installed on a general-purpose computer or a dedicated platform (appliance), which forwards or rejects/drops packets on a network. Typically firewalls are used to define zone borders. Firewalls generally have rules restricting which ports are open.

[SOURCE: ISA-62443-1-1]

3.9
identification
process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system

3.10
incident
an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies

[SOURCE: FIPS 200; SP 800-53]

3.11
integrity
guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity

[SOURCE: NIST SP 800-53]

3.12
intrusion
((still to be defined!))

3.13
IT-security
information security
cyber security
((still to be defined!))

3.14
IT-security risk
((still to be defined!))

3.15
machinery safety
((still to be defined))

3.16
password
string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization

3.17
remote access
access by users (or information systems) communicating external to an information system security perimeter

[SOURCE: NIST SP 800-53]

3.18
remote maintenance
maintenance activities conducted by individuals communicating external to an information system security perimeter

3.19
threat
any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service

[SOURCE: NIST SP 800-53]

3.20
unauthorized access
a person gains logical or physical access without permission to a network, system, application, data, or other resource

[SOURCE: NIST SP 800-61]

3.21
vulnerability
weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source

[SOURCE: NIST SP 800-53]

4 General characterization of machinery safety versus IT-security

4.1 Principle objectives

The principle objectives and conditions are very much different, see Table 1:

Table 1 — Principle objectives

	Machinery safety	**IT-Security (cyber security)**
Objectives	Injury/accident prevention, health (avoidance of harm)	Availability, integrity, confidentiality
Conditions (risks, methods, measures)	transparent (not confidential)	confidential (not shared with machinery user)
Dynamics	Rather static field (intended use, reasonable foreseeable misuse)	Highly dynamic field; moving target (intentional manipulation, criminal intent)
Risk reduction (mitigation) measures	Mainly by machine manufacture at a dedicated time (when providing the machine for the first use)	By various actors (machine manufacturer, system integrator, machine user, service provider) at any time along the overall life cycle

4.2 Different elements of risk

The elements of risk regarding safety are characterized as given in Figure 1.

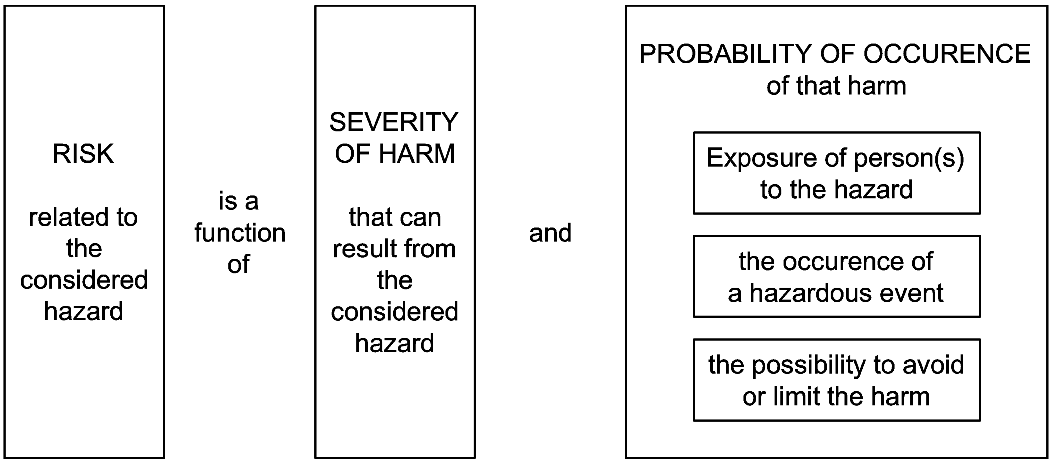
RISK
related to the considered hazard
is a function of
SEVERITY OF HARM
that can result from the considered hazard
and
PROBABILITY OF OCCURENCE of that harm
Exposure of person(s) to the hazard
the occurence of a hazardous event
the possibility to avoid or limit the harm

Figure 1 — Elements of risk related to machinery safety (see ISO 12100:2010, Figure 3)

Regarding IT-security the elements of risk are different and can be characterized according to Figure 2 as follows:

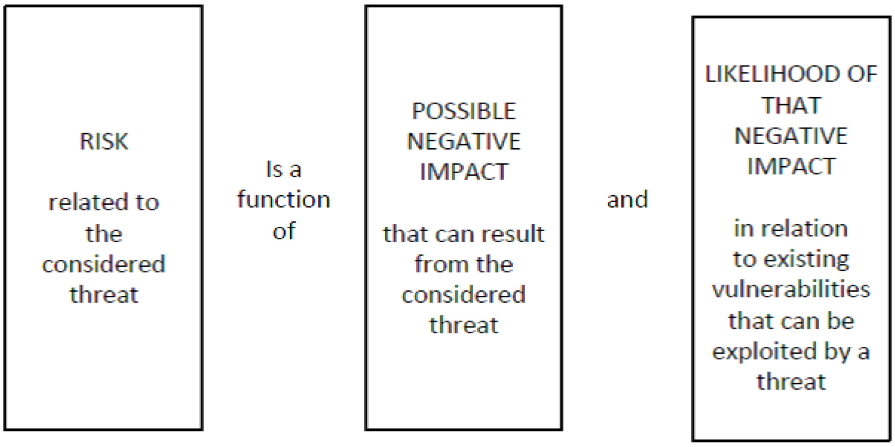
RISK
related to the considered threat
Is a function of
POSSIBLE NEGATIVE IMPACT
that can result from the considered threat
and
LIKELIHOOD OF THAT NEGATIVE IMPACT
in relation to existing vulnerabilities that can be exploited by a threat

Figure 2 — Elements of risk related to IT-security

4.3 Consequences for risk assessment process

Based on the differences shown in 4.2 risk assessment regarding machinery safety which is prescribed in ISO 12100:2010, Clause 5 has to be distinguished clearly from a risk assessment regarding IT-security.

An example regarding IT-security risk assessment for industrial automation and control systems is given in IEC/NP 62443-3-2:2015, Clause 5.

5 Relationship to existing legal and standardization framework regarding machinery safety

5.1 Legal framework

Legal frameworks for putting a machine into service the first time (responsibility of the machine manufacturers) and ISO 12100 restrict the scope of machinery safety to the “intended use” and the “reasonably foreseeable misuse” of a machine. Every kind of (external) intentional violation (sabotage/spying) of a machine is de facto a criminal act which is outside the scope of current safety legislation and consequently of standardization for machinery safety which is supporting this legislation.

EXAMPLE European Machinery Directive 2006/42/EC:

Recital (12)

“The putting into service of machinery within the meaning of this Directive can relate only to the use of the machinery itself for its intended purpose or for a purpose which can reasonably be foreseen.”

Annex I, Essential health and safety requirements relating to the design and construction of machinery

GENERAL PRINCIPLES

1. “By the iterative process of risk assessment and risk reduction referred to above, the manufacturer or his authorised representative shall:

— determine the limits of the machinery, which include the intended use and any reasonably foreseeable misuse …”

2. “The obligations laid down by the essential health and safety requirements only apply when the corresponding hazard exists for the machinery in question when it is used under the conditions foreseen by the manufacturer or his authorised representative or in foreseeable abnormal situations. …”

5.2 Standardization framework – Relationship to ISO 12100

In line with local/regional legal framework for putting machinery into service for the first time ISO 12100 does not explicitly address IT-security attacks (threats) which are categorized as intentional abuse and criminal acts.

The determination of the limits of the machinery as part of the strategy for risk assessment and risk reduction in ISO 12100 only considers the intended use and any reasonably foreseeable misuse (see ISO 12100:2010, Clause 4). IT-security attacks (threats) from outside and possible safety implications (via vulnerabilities of the machine control system or other electronic parts) are not considered as reasonably foreseeable misuse.

However, manufacturers providing machinery which can have vulnerabilities to IT-security attacks (threats) should take this aspect into account in particular when IT security attacks (threats) can have an impact to machinery safety.

6 Relationship between machinery safety and IT-security

The relationship between machinery safety and IT-security in shown in Figure 3.

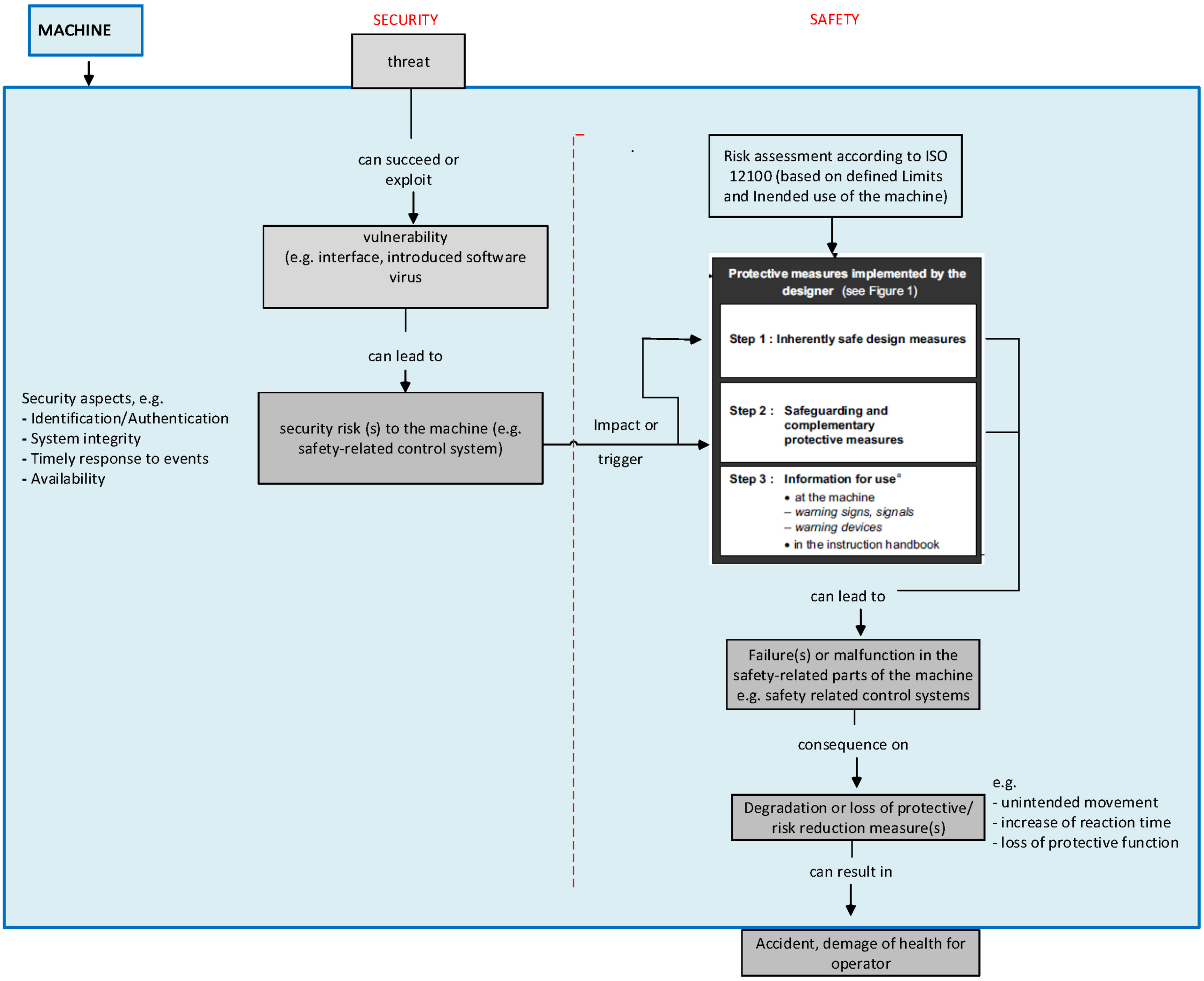
MACHINE
SECURITY
SAFETY
threat
can succeed or exploit
vulnerability (e.g. interface, introduced software virus
can lead to
security risk (s) to the machine (e.g. safety-related control system)
Security aspects, e.g.
- Identification/Authentication
- System integrity
- Timely response to events
- Availability
Impact or trigger
Risk assessment according to ISO 12100 (based on defined Limits and Inended use of the machine)
Protective measures implemented by the designer (see Figure 1)
Step 1 : Inherently safe design measures
Step 2 : Safeguarding and complementary protective measures
Step 3 : Information for use[a]
• at the machine
– warning signs, signals
– warning devices
• in the instruction handbook
can lead to
Failure(s) or malfunction in the safety-related parts of the machine e.g. safety related control systems
consequence on
Degradation or loss of protective/ risk reduction measure(s)
e.g.
- unintended movement
- increase of reaction time
- loss of protective function
can result in
Accident, demage of health for operator

Figure 3 — Relationship between machinery safety and IT-security

Resulting from 4.3 and Figure 3 the safety risk assessment for a machine according to ISO 12100 should be made in advance of any IT-security risk considerations. The resulting

— inherently safe design measures, and

— safeguarding and protective/risk reduction measures

of a machine should then be analysed regarding possible vulnerabilities against IT-security attacks (threats).

A machine provided without any interface for external IT communication shall be considered safe against IT-security threats (attacks).

7 Essential steps to address IT-security in general

IT-security threats and vulnerabilities require cooperation and coordination between the component suppliers, the machinery manufacturer, the system integrator, and the machinery user. Each has a role to play in preventing IT-security attacks throughout the phases of the lifecycle of the machinery. No party can assign to, or assume that, another party is fully responsible for IT-security. At the same time, no party has all of the required information available to effectively address IT-security threats and vulnerabilities throughout the phases of the lifecycle of the machinery.

Component suppliers, the machinery manufacturer, the system integrator, and the machinery end user should each use the essential elements to evaluate its system(s). Part of the evaluation should include communicating to the other parties the threats and vulnerabilities which it cannot fully address alone or which have implications to the other parties. For example, a machine manufacturer cannot prevent an IT-security threat if the machinery user connects the machine to the connected world via its communication or networked system. The machinery manufacturer should inform the machinery user of the preferred communications method(s) in order to minimize potential attacks.

Essential steps for providing effective IT-security should be considered by machinery manufacturers and system integrators. This should be done as far as possible in the context of the machinery user's actual or expected IT-infrastructure.

The following five steps should enable machinery manufacturers and system integrators – regardless of size, degree of IT-security threats, or sophistication – to apply the principles and best practices to improving the security and resilience of machine control systems. The steps provide organization and structure to today's multiple approaches to IT-security threats by assembling standards, guidelines, and practices that are working effectively in industry today.

These steps provide the ongoing process of identifying, assessing, and responding to risk. Machinery manufacturers and system integrators should understand the likelihood of an attack and the resulting impact. With this information, machinery manufacturers and system integrators can determine the acceptable level of risk for machine control systems.

The following steps are essential and shall be addressed to provide effective IT-security for machinery.

Depending on the application, several of these steps may not be addressed by the machine manufacturer and system integrator but in the first instance by the machine user.

a) **Identify** – What are the IT security threats and vulnerabilities?

- Understanding why would an entity attack the machine control system?
- What does the machine user have that is valuable?
- What are the vulnerabilities of the machine (e. g. open ports/external interfaces)?
- What are the resources that support critical functions?

For example,

- critical infrastructure – utilities, IT network (asset management),
- risk assessment, risk management strategy (governance),
- access control,
- data security,
- information protection processes and procedures,

- awareness and training,
- protective technology.

b) **Protect** – Develop and implement the appropriate counter measures to protect the machine.

The counter measures support the ability to prevent, limit or contain the impact of a potential IT-security attack. Examples of counter measures include machine control system design, internet access, access control, awareness and training, data security, information protection processes and procedures, maintenance and protective technology (see [7]).

c) **Detect** – Develop and implement the appropriate measures to identify the occurrence of an IT-security attack.

The "detect"-element enables timely discovery of IT- security attacks. Examples include anomalies and events, security continuous monitoring and detection processes.

d) **Respond** – Develop and implement the appropriate activities to take action regarding a detected IT-security attack.

The "respond"-element supports the ability to stop and or contain the impact of a potential IT-security attack. Examples include mitigation, response planning, communications, analysis and improvements.

e) **Recover** – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to an IT-security attack.

The "recover"-element supports timely recovery to normal operations to reduce the impact from an IT-security attack. Examples include recovery planning, improvements and communications.

NOTE For further guidance see also [1].

8 Generic guidance for assessing IT-security threats regarding their possible influence on machinery safety

There exist some typical motivations resulting in IT-security threats related to machinery. If these threats successfully exploit vulnerabilities of a machine, their relevance for machinery safety varies significantly. Table 2 shows four cases of unauthorized access which require consideration.

Table 2 — IT security threats and motivations

Case	IT security threat	Manipulation of the machinery and plant	Relevance for machinery safety
1	Access to data/know-how from the machine manufacturer or from the machine user (process know-how)	None	None
2	Creation of economic damage to the machine user	During use	Unlikely but possible
3	Creation of hazard of machinery and/or people (operator, bystanders)	During use	Unlikely but possible
4	Creation of damage to infrastructure and/or people (operator; bystanders), e.g. a terroristic act	During use	Yes

For cases 1 and 2 the intentional (extern) violation is often hidden and, therefore, difficult to detect even after the intrusion. For cases 3 and 4 the violation can remain hidden after the intrusion.

Case 4 has a much higher probability of occurrence for machinery and especially for plant used in so called critical infrastructures (generation of electric power, water supply etc.) compared to other machinery and plant intended for "normal" manufacturing purposes.

Based on such a generic assessment of the overall portfolio of IT security threats, those threats can be identified which need further consideration regarding safety of machinery.

9 Roles to address IT-security issues with possible relevance to machinery safety

IT-security risks which may have an influence on machine safety are constantly evolving during the whole life cycle of a machine. The same applies for the appropriate/necessary counter-measures.

Considering the above mentioned life cycle of a machine Table 3 allocates different roles to the machine manufacturer, to the system integrator and to the end user of a machine/machine system for initiating appropriate/necessary counter-measures. There might be additional protective areas and protective measures depending on the particular way how a machine will be installed and used which are not considered in Table 3. Depending on the contractual base among the three actors the allocation of roles (listed protective measures) to the individual actor(s) might be different.

Table 3 — Examples for protective measures to avoid/restrict IT-security threats which can have influence on machine safety

Protective area	Protective measure	Machine manu-facturer	System integrator	End user
Restriction of logical/physical access to the IT-system (with possible influence on safety)	Separation of safety relevant IT-system from overall IT-system	x	x	
	Provision of IT-system with protective measures (e.g. firewalls, antivirus tools)	x	x	
	Preservation of the protective measures of the IT-system in an actual secure mode (e.g. update of antivirus tools)			x
	Provision of separate authentication and access control mechanisms (e.g. card readers, physical locks)	x	x	
	Provision of a network topology with multiple and independent layers	x	x	
	Restriction of IT-system user privileges to only those that are required for each person's role			x
	Disabling of all unused ports and services			x
	Responsibility for individual user accounts and the account management (e.g. update of passwords)			x
	Provision of the machine with means for an authorization check of the players/services	x	x	

	after every authentication			
	Provision of the machine with physical hardware measures to bring it into safe state in the case of a severe security attack. (e.g. emergency stop, shut down button)	x	x	
	Physical restriction of access or use of IT connection points (e.g. USB or Ethernet sockets)	x	x	x
	Disconnection or deactivation of accessible IT connection points (e.g. USB or Ethernet sockets)	x	x	x
	Observation of instructions for use of component manufacturers regarding — the use of IT connection points, — the phase of the life cycle of the machine in which the connection is required, — the duration of the required connections, — the IT interface (HW/SW) specified by the component manufacturer, — the access restriction to the application SW specified or recommended by the component manufacturer.	x	x	x
Detection and reaction on security events and incidents (with possible influence on safety)	Provision of the machine with capability to detect failed IT-system components or unavailable services	x	x	
	Provision of the machine with means for monitoring of vulnerabilities	x	x	
	Responsiveness and reaction to vulnerabilities			x
In the case of remote maintenance and service	Provision of means for setting up and ending of a remote access session The means shall be provided on the machine and have priority over remote access commands. If reasonably possible this means shall be independent of software so that they cannot by bypassed remotely.	x	x	
	Monitoring of any remote access session (restriction of duration for remote access)			x
	Means for use of encryption for initiating a remote maintenance/remote service	x	x	

10 Guidance for machine manufacturers to address IT-security issues with possible relevance to machinery safety

10.1 General

IT-security risks which may have an influence on machine safety are constantly evolving during the whole life cycle of a machine. The same applies for the appropriate/necessary counter-measures.
Within this context the influence of the machine manufacturer is basically concentrated on measures relevant at the life cycle stage "putting the machine into service the first time". This requires in particular to incorporate in the machine those machine parts/components, which can be targets for IT-security risks (hardware and software), with certain state of the art features which can be helpful to avoid/restrict those risks (threats) as well as a design of the entire machine according to state of the art principles regarding IT-security.

Apart from those direct measures regarding originally installed hardware and software as well as appropriate design of the entire machine regarding IT-security, the significant contribution by the machine manufacturer can be made by appropriate information on the vulnerability analysis in its instruction handbook to the customer/end user (and possibly to the system integrator).

10.2 Selection of appropriate components (hardware/software)

Safety related machine parts/components (e.g. control systems, sensors, actuators) which can be targets for IT-security risks (threats) should have state-of-the-art features, which can minimize their vulnerability against those possible threats. For example,

— means/measures for identification and/or authentication for access control (e. g. card readers, physical locks, password-systems),

— means for software upgradability,

— *((possible further concrete means based on IEC 62443-4-2; to be checked)).*

10.3 Appropriate machine design

At the design stage the machine manufacturer should observe basic principles/measures to minimize the vulnerability of safety-related parts of the entire machine with regard to IT security threats. For example:

— Separate safety-relevant IT-system as far as possible from the overall IT-system of the machine.

— Equip the machine IT-system with protective measures (e.g. firewalls, antivirus tools).

— Reduce the complexity of the machine IT-system (allows a better addressing of possible IT security threats).

— Realize a machine IT-system topology with multiple and independent layers (reducing vulnerability).

— Equip the machine with means to detect failed IT-system components being essential for safety or unavailable protective/risk reduction measures.

— Equip the machine with means which brings the machine in case of a failed IT-system component being essential for safety or unavailable protective/risk reduction measures ultimately to a safe state.

— *((possible further concrete means based on IEC 62443-3-3; to be checked))*

10.4 Instruction handbook (guidance to the machine user)

As stated in Clause 7 addressing IT-security issues successfully require cooperation between various stakeholders among them machine manufacturers and machine users. The preferred means to provide guidance (recommendations) from the machine manufacturer to the machine user with regard to potential IT-security aspects in relation to machinery safety is the instruction handbook.

The instruction handbook should contain appropriate guidance/recommendation how to address IT-security issues during the machine use in relation to the means/measures provided by the machine (component) manufacturer with regard to potential IT-security aspects in relation to machinery safety.

For example:

a) Restriction of logical/physical access to IT systems (with possible influence on safety)

1) Use internal IT systems with protective measures (e. g. firewalls, antivirus tools).
2) Keep the protective measures of the IT system in an actual secure mode (implement updates from machine/component manufacturers).
3) Use provided authentication and access control mechanism (e. g. card readers, physical locks) according to the specifications of the machine/component manufacturer.
4) Restrict IT system user privileges only to those that are required for each person´s role.
5) Disable all unused external ports/interfaces and services.
6) Introduce an individual user account and the related account management (e. g. update of passwords).
7) Use provided means for an authorization check of the players/services after every authentication according to the specifications of the machine/component manufacturer.

b) Detection and reaction on IT-security events and incidents (with possible influence on safety)

1) Check regularly provided means for detecting failed IT system components or unavailable service according to the specifications of the machine/component manufacturer.
2) Be responsive and reactive for new vulnerabilities (resulting from an IT security attack (threat)).

c) In case of remote maintenance and service

1) - using provided means for setting up and ending a remote access session according to the specifications of the machine/component manufacturer
2) - using means of encryption for initiating a remote maintenance/remote service according to the specifications of the machine/component manufacturer
3) - watching any remote access session (restriction of duration for remote access)

Parking lots to be deleted or incorporated in Clause 10

PARKING LOT 1: Copied in from "old" 6.1:

Implementing the essential elements should include the following actions:

1) Document the current profile of the machine control system with respect to IT security
2) Conduct a risk assessment of the machine in accordance with ISO 12100
3) Document the desired state of the machine control system
4) Determine, analyze and prioritize the gaps
5) Implement an action plan to get to the desired state.

NOTE For additional details on IT-security aspects for machinery safety see IEC 62443 and CENELEC Guide 32:2014, A.8.

PARKING LOT 2: Last three paragraphs from "old" Clause 4:

Another aspect which should be considered is that IT-security threats and vulnerabilities are constantly changing/evolving during the life time of a machine. Therefore, they cannot be satisfactorily covered by the machine manufacturer once the machine has been put into service for the first time, and countermeasures should also evolve to address these threats and vulnerabilities.

Machine parts/components including hardware and software can be targets for IT-security threats and vulnerabilities. The machine manufacturer can select machine parts/components with certain basic features which can be helpful to avoid/restrict those threats and vulnerabilities (e. g. means/measures for identification and/or authentication). However, a major contribution by the machine manufacturer when putting the machine into service for the first time is the provision of appropriate recommendations in the information for use.

The machine manufacturer should consider the IT-security threats and vulnerabilities which can influence machinery safety. This should be done as far as possible in cooperation with the machine user. The evaluation should consider the overall assessment of IT-security threats and vulnerabilities covering all relevant motivations and related ways of intentional (extern) violation.

PARKING LOT: "Old" subclauses 6.3.1 to 6.3.3:

General

IT security risks can be mitigated through the combined efforts of component suppliers, the machinery manufacturer, the system integrator, and the machinery end user. In general, there are several potential responses to security risks:

a) design the security risk out (avoid vulnerabilities);

b) reduce the security risk (prevent threats and limit vulnerabilities);

c) accept the security risk;

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

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

Flow chart

The following flow chart *((still to be provided by David Reade and Patrick Gehlen))* provides guidance on the step by step approach to limiting or restricting IT security threats and vulnerabilities.

1) Does it need to be connected?

2) Does it need to be connected at all times (continuously)?

3) Is the connection monitored?

4) Is the connection monitored and configurable?

5) Video observation of process without ability to change

Recommendations/Guidance

The following list provides practical guidance on the basics of IT security that component suppliers, systems integrators, machinery manufacturers and end users may use to improve their machinery or systems.

NOTE This list is in no particular order.

a) Reference to pertinent standards.

b) Turn on passwords and antivirus tools.

c) The initial default password should be changed at installation, and frequently changed thereafter.

d) Isolating the lines of communication for safety relevant communications from those that are not safety relevant such as segmenting operations into functional sub-networks with more firewalls

e) Separate device and production networks from enterprise/business networks and the Internet with managed Ethernet switches used as firewalls.

f) Determine if connecting a machine is necessary or needed. If not necessary, consider disconnecting the machinery from the web.

g) Consider restricting data flows to be one directional (outgoing only) such as enabling read-only functions that allow operations to send out data, but prohibit any incoming instructions or commands.

h) Physical restriction of access or use of IT connection points (e.g. USB or Ethernet sockets)

i) Disconnection or deactivation of accessible IT connection points (e.g. USB or Ethernet sockets)

j) Consider limiting incoming access to specific times or individuals rather than leaving the lines continuously open:

— an arranged rendezvous between two people.

k) Use the Security Risk Mitigation (Reduction) Flow chart.

l) Develop a Security Risk Mitigation (Reduction) Plan.

m) Instructions for use to convey to machinery user.

- IEC 62443

n) Observation of instructions for use of component manufacturers

o) For machinery itself and for the components selected/used

p) For component manufacturer

q) Control who has access to application or network:

- Physically?
- Who has access?

r) Ensure a robust reliable operation - firewalls

s) Protect - antivirus

t) Patch – update firmware

u) Adopt and follow appropriate software patching policies

v) Develop – security policies

w) Implementation – key switch to run

x) Monitor – change detection

y) Limit access – physical restriction

z) IT and safety culture for implementation and ongoing maintenance

aa) Train and retrain staff to follow agreed upon security procedures

bb) Establish regularly scheduled network traffic evaluation using IT based software tools that can identify, disallow and purge unauthorized probes and intrusions.

cc) Observation of instructions for use of component manufacturers regarding:

- The use of IT connection points
- The phase of the machine life in which the connection is required
- The duration of the required connections.
- The IT interface (HW/SW) specified by the component manufacturer

  - The access restriction to the application SW specified or recommended by the component manufacturer

Examples of methods used to prevent IT security vulnerabilities from unauthorized access and modification include:

- human user identification and authentication;
- authentication for networks;
- software account management;
- wireless access management;
- strength of password-based authentication;
- password generation and access restrictions;
- designing systems to be resistant to casual or coincidental IT-security violations such as caused by inadvertent human error by automatically shutting down connections after a certain timeperiod of inactivity when an authorized person forgets to logout of an access port.

NOTE Human error can have little relation to IT-security in its strict sense. Those (internal) unintentional influences (reasonably foreseeable human error when operating the control system) **have to be considered** already within the normal (safety-related) risk assessment and the resulting inherent safe design of the control system (see ISO 12100:2010, 6.2.11.1). Therefore no further consideration is necessary at the level of machinery safety standardization.

Bibliography

[1] *Capabilities Assessment for Securing Manufacturing Industrial Control Systems* Draft Nov 2016 - https://nccoe.nist.gov/sites/default/files/library/project-descriptions/mf-ics-1-project-description-draft.pdf

[2] CNSSI-4009, *((title to be added))*

[3] FIPS 200, *((title to be added))*

[4] ISA-62443-1-1, *((title to be added))*

[5] NIST SP 800-53, *((title to be added))*

[6] NIST SP 800-61, *((title to be added))*

[7] NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security*, Revision 2, May 2015. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-109 82r2.pdf

[8] RFC 4949, *((title to be added))*

[9] ISO/IEC 20924, *((title to be added))*

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

[11] IEC 62443-3-2:2015[1], *Industrial communication networks - Network and system security - Part 3-2: Security levels for zones and conduits*

[12] IEC 62443-3-3, *Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels*

[13] IEC 62443-4-2, *((title to be added))*

[14] CENELEC Guide 32: *Guidelines for Safety Related Risk Assessment and Risk Reduction for Low Voltage Equipment*

[1] In preparation.