TECHNICAL REPORT

ISO/TR 22100-4

First edition
2018-12

Safety of machinery — Relationship with ISO 12100 —

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

Reference number
ISO/TR 22100-4:2018(E)

© ISO 2018

COPYRIGHT PROTECTED DOCUMENT

© ISO 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

 © ISO 2018 – All rights reserved

Contents

Page

© ISO 2018 – All rights reserved

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 of the voluntary nature of standards, 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 www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 199, *Safety of machinery*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

A list of all parts in the ISO 22100 series can be found on the ISO website.

© ISO 2018 – All rights reserved

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, the foundations are vertical networking and horizontal integration across the entire value chain, convergence of design, ordering, delivery and manufacturing capabilities. This results in the transformation of conventional value chains and the emergence of new business models. Smart products based on smart manufacturing know many details on how they were made, their performance and how they are being used. The physical product is linked to its digital representation, and the digital content depends on lifecycle phase. Implementing smart manufacturing creates 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 leads to the emergence of dynamic, real-time optimized, self-organizing value chains. An appropriate regulatory framework is therefore necessary, 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.

For smart manufacturing, the description of the network infrastructure needs to be further expanded 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 aspects on safety of machinery that can be affected by IT-security attacks related to the direct or remote access to, and manipulation of, a safety-related control system(s) by persons for intentional abuse (unintended uses). IT-security attacks are increasingly becoming a potential threat to the safety of machinery. Although intentional abuse falls outside the scope of ISO 12100 and the (safety-related) risk assessment process, it is reasonable also for machinery manufacturers to consider such threats.

Current technologies enable machinery to be monitored and/or improved regarding their 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 persons with nefarious or criminal intent to make adjustments that can put workers and others at risk of harm. For example, speeds or forces can be adjusted to dangerous levels, temperatures can be lowered below a kill step level resulting in food contamination, or error codes or messages can be erased or falsified.

Human error can have little relation to IT-security in its strict sense. Those unintentional influences (reasonably foreseeable human error when adjusting parameters of the machine or its control system) are already covered within the normal (safety-related) risk assessment and the resulting inherently safe design of the control system (see ISO 12100:2010, 6.2.11.1).

© ISO 2018 – All rights reserved

Safety of machinery — Relationship with ISO 12100 —

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

1 Scope

This document gives machine manufacturers guidance on potential security aspects in relation to safety of machinery when putting a machine into service or placing on the market for the first time. It provides essential information to identify and address IT-security threats which can influence safety of machinery.

This document gives guidance but does not provide detailed specifications on how to address IT-security aspects which can influence safety of machinery.

This document does not address the bypass or defeat of 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:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
antivirus tool
software used to detect malicious code, prevent it from infecting a system, and remove malicious code that has infected the system

3.2
attack
attempt to gain unauthorized access to system services, resources, or information

[SOURCE: CNSSI-4009, modified — "., or an attempt to compromise system integrity, availability, or confidentiality" has been deleted at the end of the definition.]

© ISO 2018 – All rights reserved

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 permission that is granted to a system entity to access a system resource

[SOURCE: RFC 4949]

3.5
confidentiality
preserving authorized restrictions on, and preventing *unauthorized access* (3.18) to information

3.6
encryption
transformation of data into a form 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 — The word "cryptographic" has been deleted before "transformation of data" and "(called "plaintext")" deleted afterwards; "(called "ciphertext")" has been deleted after "form". The second sentence has been moved to Note 1 to entry.]

3.7
firewall
software that restricts data communication traffic between two connected networks.

Note 1 to entry: It is also common to name specific hardware in which the software runs a firewall.

3.8
integrator
entity who designs, provides, manufactures or assembles an integrated manufacturing system and is in charge of the safety strategy, including the protective measures, control interfaces and interconnections of the control system

Note 1 to entry: The integrator can be a manufacturer, assembler, engineering company or the user.

[SOURCE: ISO 11161:2007, 3.10]

3.9
integrity
condition of guarding against improper modification or destruction of information

3.10
IT-security
Information Technology security
cyber security
protection of an IT-system from the *attack* (3.2) or damage to its hardware, software or information, as well as from disruption or misdirection of the services it provides

3.11
IT-security incident
occurrence that actually or potentially jeopardizes the *confidentiality* (3.5), *integrity* (3.9), or availability of an IT-system

© ISO 2018 – All rights reserved

3.12
machine control system
system which responds to input signals from parts of machine elements, operators, external control equipment or any combination of these and generates output signals causing the machine to behave in the intended manner

Note 1 to entry: The machine control system can use any technology or any combination of different technologies (e.g. electrical/electronic, hydraulic, pneumatic, mechanical).

[SOURCE: ISO 13849-1:2015, 3.1.32]

3.13
password
string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access *authorization* (3.4)

3.14
remote access
access by users (or information systems) communicating external to an information system security perimeter

[SOURCE: NIST SP 800-53]

3.15
risk reduction measure
protective measure
action or means to eliminate hazards or reduce risks

[SOURCE: ISO/IEC Guide 51:2014, 3.13]

3.16
smart manufacturing
manufacturing that improves its performance aspects with integrated and intelligent use of processes and resources in cyber, physical and human spheres to create and deliver products and services, which also collaborates with other domains within enterprises' value chains

Note 1 to entry: Performance aspects include agility, efficiency, safety, security, sustainability or any other performance indicators identified by the enterprise.

Note 2 to entry: In addition to manufacturing, other enterprise domains can include engineering, logistics, marketing, procurement, sales or any other domains identified by the enterprise.

3.17
threat
any *IT-security incident* (3.11) with the potential to adversely impact machinery operations

3.18
unauthorized access
any logical or physical access which is not intended by the owner of an IT-system

3.19
vulnerability
weakness in the security of an IT-system that can be exploited or triggered by a *threat* (3.17)

4 General characterization of safety of machinery versus IT-security

4.1 Principle objectives

The principle objectives and conditions of IT-security are very much different from machinery safety, see Table 1.

© ISO 2018 – All rights reserved

Table 1 — Principle objectives

	Safety of machinery	IT-Security (cyber security)
Objectives	injury/accident prevention, health (avoidance of harm)	availability, integrity, confidentiality
Conditions (risks, methods, measures)	transparent (obvious)	not obvious (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 manufacturer at a dedicated time (when providing the machine for the first use)	by various actors (machine manufacturer, 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.

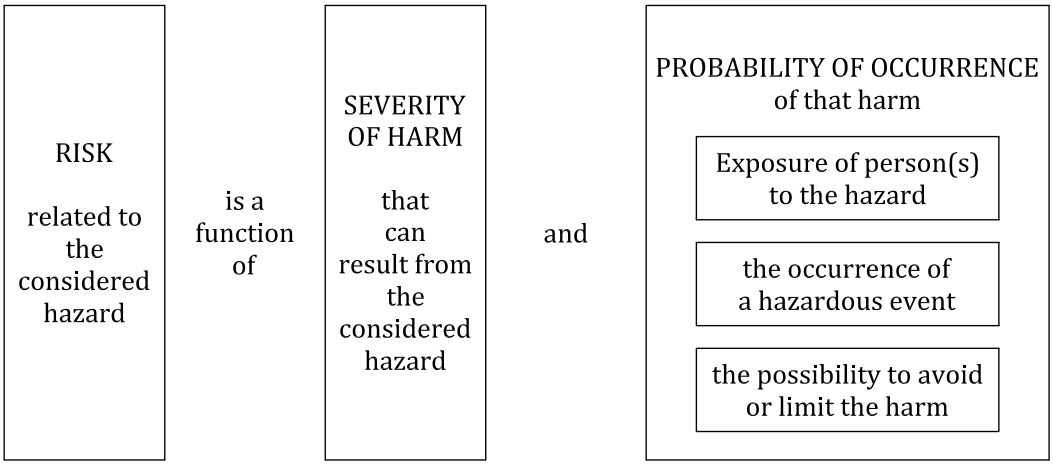

Figure 1 — Elements of risk related to safety of machinery (see ISO 12100:2010, Figure 3)

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

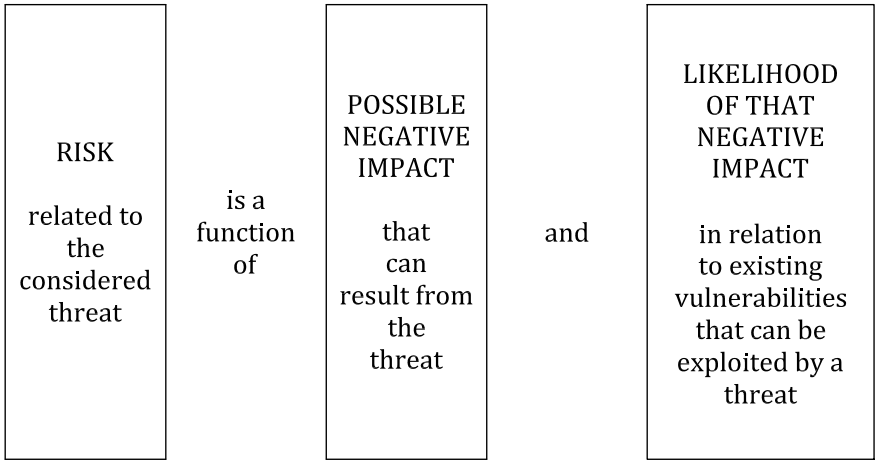

Figure 2 — Elements of risk related to IT-security

© ISO 2018 – All rights reserved

4.3 Consequences for risk assessment process

Based on the differences shown in 4.2, risk assessment regarding safety of machinery 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 62443-3-2:—[1)], Clause 5.

5 Relationship to existing legal and standardization framework regarding safety of machinery

5.1 Legal framework

Legal frameworks for putting a machine into service or placing it on the market for the first time (responsibility of the machine manufacturers) and ISO 12100 restrict the scope of safety of machinery to the "intended use" and the "reasonably foreseeable misuse" of a machine. Every kind of intentional violation (sabotage/spying) of a machine is de facto a criminal act which is outside the scope of current safety legislation. Consequently, it is also out of the scope of standardization for safety of machinery, which supports such legislation. For an example, see Annex A.

5.2 Standardization framework – Relationship to ISO 12100

In line with local/regional legal framework for putting machinery into service or placing on the market for the first time, ISO 12100 does not explicitly address IT-security attacks and/or 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 and/or 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 and/or threats should take this aspect into account in particular when IT-security attacks and/or threats can have an impact to safety of machinery.

6 Relationship between safety of machinery and IT-security

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

1) Currently available as draft document IEC 65/690/CDV:2018.

© ISO 2018 – All rights reserved

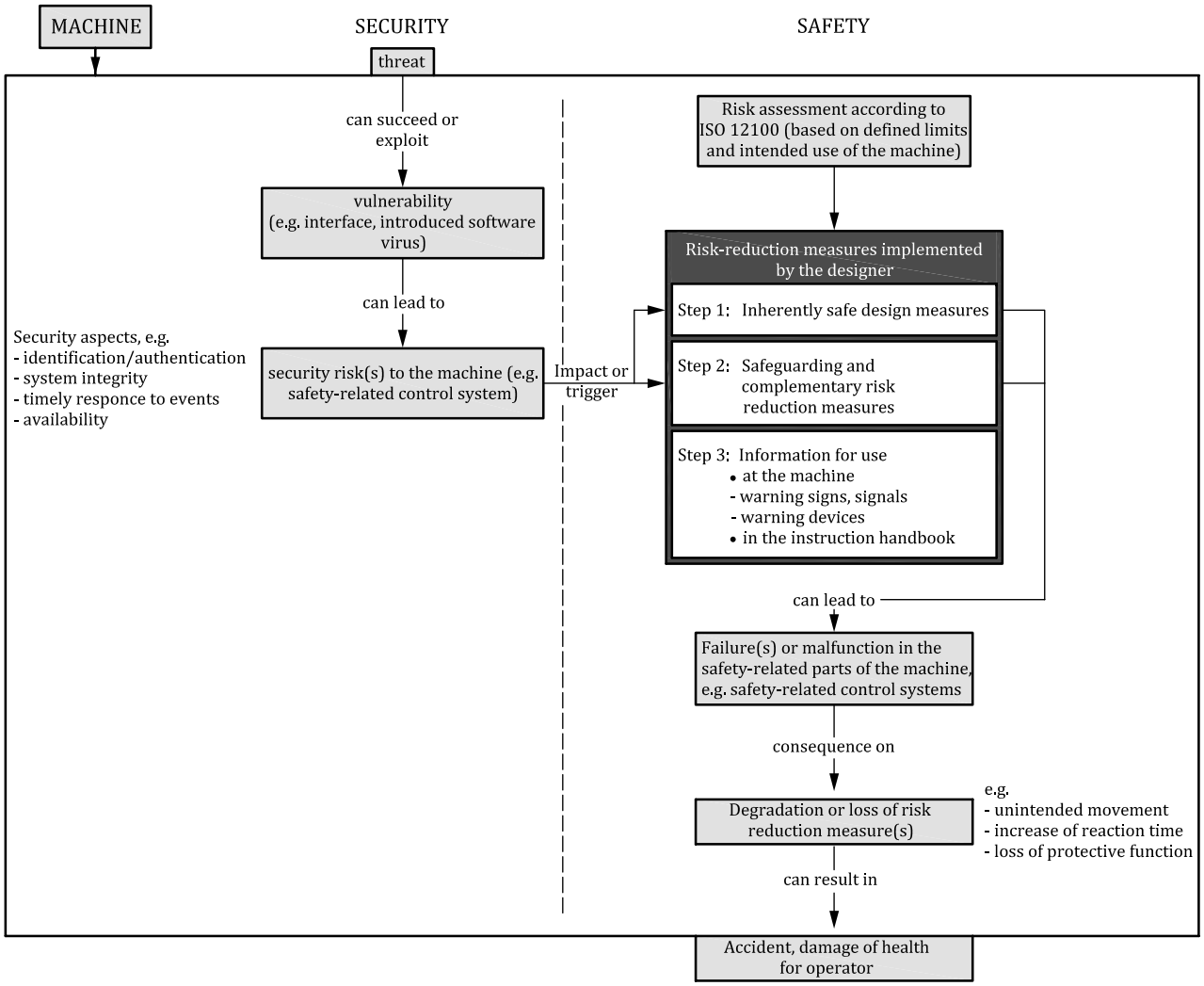

Figure 3 — Relationship between safety of machinery and IT-security

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 risk reduction measures, of a machine should then be analysed regarding possible vulnerabilities against IT-security threats.

Resulting IT-security risks can then be mitigated through the combined efforts of component suppliers, the machinery manufacturer, the integrator, and the machinery user. In general, the potential responses to security risks should apply the following hierarchy based on ISO 12100:

a) eliminate the security risk by design (avoid vulnerabilities);

b) mitigate the security risk by risk reduction (mitigation) measures (limit vulnerabilities);

c) provide information about the residual security risk and the measures to be adapted by the user.

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

Those vulnerabilities against IT-security attacks (threats) depend heavily on whether a machine can be connected to an external IT-system and how often this happens. Answering the following questions can help limit or restrict IT-security threats and vulnerabilities.

1) Does it need to be connected?

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

 © ISO 2018 – All rights reserved

3) Is the connection monitored [e.g. using a virtual private network (VPN) system]?

4) Is the connection configurable (e.g. access for authorized persons only)?

5) Can the connection be restricted to "read only" mode (without ability to change)?

Consequently, a machine without any direct or indirect interface to external IT-systems can be considered as not vulnerable to IT-security attacks.

7 Essential steps to address IT-security over the whole life cycle of the machine

IT-security threats and vulnerabilities require cooperation and coordination between the component suppliers, the machinery manufacturer, the 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 another the responsibility for IT-security, or assume that another 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 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 entirely 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 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 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 machinery.

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

   — 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?

   Examples include 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 and 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 [16]).

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 IT-security incidents, security continuous monitoring and detection processes.

© ISO 2018 – All rights reserved

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 [10].

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 (threats). Machinery manufacturers and integrators in co-operation with the machine user can estimate the likelihood of an attack and the resulting impact.

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

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

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

Table 2 — IT-security threats and motivations

Case	IT-security threat	Manipulation of the machinery and plant	Relevance for safety of machinery
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 for 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	Likely

NOTE Access to an IT-system can also result in unintended consequences.

For all cases the intentional violation can remain hidden and, therefore, difficult to detect even after a successful attack.

Case 4 has a much higher risk (threat) for machinery and especially for plant used in critical infrastructures (generation of electric power, water supply etc.) compared to other machinery and plant 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.

© ISO 2018 – All rights reserved

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

IT-security risks which can have an influence on machine safety constantly evolve during the 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 integrator and to the end user of a machine/machine system for initiating appropriate/necessary counter-measures. There can be additional protective areas and risk reduction measures depending on the particular way a machine is installed and used which are not considered in Table 3. Depending on the contractual base among the three entities, the allocation of roles [listed risk reduction (mitigation) measures] to the individual actor(s) can be different.

Table 3 — Examples for risk reduction (mitigation) measures to avoid/restrict IT-security threats which can have influence on safety of machinery

Protective area	Risk reduction (mitigation) measure	Machine manufacturer	Integrator	End user
Restriction of logical/physical access to the IT-system (with possible influence on safety)	Physical separation of safety relevant IT-system from overall IT-system	x	x	x
	Provision of IT-system with risk reduction (mitigation) measures (e.g. firewalls, antivirus tools)	x	x	x
	Preservation of the risk reduction (mitigation) measures of the IT-system in an actual secure mode (e.g. update of antivirus tools)			x
	Provision of means allowing a software upgrade	x	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

© ISO 2018 – All rights reserved

Table 3 *(continued)*

Protective area	Risk reduction (mitigation) measure	Machine manufacturer	Integrator	End user
	Provision of the machine with means for an authorization check of the players/services after every authentication	x	x	
	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, — the use of (turn on) passwords and antivirus tools, — changing the initial default password at installation, and frequently after that.	x	x	x
Detection and reaction on IT-security 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

© ISO 2018 – All rights reserved

Table 3 *(continued)*

Protective area	Risk reduction (mitigation) measure	Machine manufacturer	Integrator	End user
In the case of remote maintenance and service	Provision of means for setting up and ending of a remote access session Provision of means on the machine that have priority over remote access commands Provision of means independent of software so that they cannot be bypassed remotely Provision of incoming access limits to specific times or individuals rather than leaving the lines continuously open (an arranged rendezvous between two people)	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 safety of machinery

10.1 General

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

In this context, the influence of the machine manufacturer is basically concentrated on measures relevant at the life cycle stage "putting the machine into service or placing on the market for the first time". This requires incorporating machine parts/components, which can be targets for IT-security risks (hardware and software) with certain state-of-the-art features that can be helpful to avoid/ restrict those risks (threats).

In addition to those direct measures regarding originally installed hardware and software as well as appropriate design of the entire machine regarding IT-security, a 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 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 authentication for access control (e. g. card readers, physical locks, password-systems);

— means for software integrity;

— means for data integrity;

— means for software upgradability;

© ISO 2018 – All rights reserved

— means for encrypted communication.

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 risk reduction (mitigation) 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 risk reduction (mitigation) measures;

— equip the machine with means/measures for authentication for access control (e.g. card readers, physical locks, password-systems);

— equip the machine with means for software upgradability;

— equip the machine with means which brings the machine to a safe state in case of a failed IT-system component being essential for safety or unavailable risk reduction (mitigation) measures.

10.4 Instruction handbook (guidance to the machine user)

As stated in Clause 7, addressing IT-security issues successfully requires 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 safety of machinery is the instruction handbook.

The instruction handbook should include information from 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 (hardware/software) specified;

— the access restriction to the application software specified or recommended.

The instruction handbook should include information about the required training and retraining of staff to follow IT-security procedures.

The instruction handbook should contain appropriate guidance/recommendations on how to address IT-security issues during the machine use. The instructions should take into account the means/measures provided by the machine (component) manufacturer with regard to potential IT-security aspects as related 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 risk reduction (mitigation) measures (e.g. firewalls, antivirus tools);

   2) keep the risk reduction (mitigation) measures of the IT-system in an actual secure mode (implement updates from machine/component manufacturers);

 © ISO 2018 – All rights reserved

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 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) use provided means for setting up and ending a remote access session according to the specifications of the machine/component manufacturer;

2) use means of encryption for initiating a remote maintenance/remote service according to the specifications of the machine/component manufacturer;

3) watch any remote access session (restriction of duration for remote access).

© ISO 2018 – All rights reserved

Annex A
(informative)

Example of a legal framework

EXAMPLE European Machinery Directive 2006/42/EC:

Recital (12)

"The putting into service or placing on the market 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****. ..."*

© ISO 2018 – All rights reserved

Bibliography

[1] ISO/IEC Guide 51:2014, *Safety aspects — Guidelines for their inclusion in standards*

[2] ISO 11161:2007, *Safety of machinery — Integrated manufacturing systems — Basic requirements*

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

[4] ISO/IEC 20924[2)], *Information technology — Internet of Things (IoT) — Definition and vocabulary*

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

[6] IEC 62443-3-2:— [3)], *Security for industrial automation and control systems — Part 3-2: Security risk assessment and system design*

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

[8] IEC 62443-4-2, *Industrial communication networks — Security for industrial automation and control systems — Part 4-2: Technical security requirements for IACS components*

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

[10] *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

[11] CNSSI-4009, Committee on National Security Systems (CNSS) Glossary, April 2015, USA https://cryptosmith.files.wordpress.com/2015/08/glossary-2015-cnss.pdf

[12] FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems,* Federal Information Processing Standards Publication, March 2006, USA http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

[13] NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations,* Revision 4, April 2013 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[14] NIST SP 800-61, *Computer Security Incident Handling Guide,* Revision 2, August 2012 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[15] 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

[16] RFC 4949, *Internet Security Glossary*, Version 2, August 2007

2) Under preparation. (Stage at the time of publication: ISO/IEC CD 20924.)

3) Currently available as draft document IEC 65/690/CDV:2018.

© ISO 2018 – All rights reserved

ICS 13.110
Price based on 15 pages

© ISO 2018 – All rights reserved