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 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

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 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.

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).

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.]

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

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.

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.

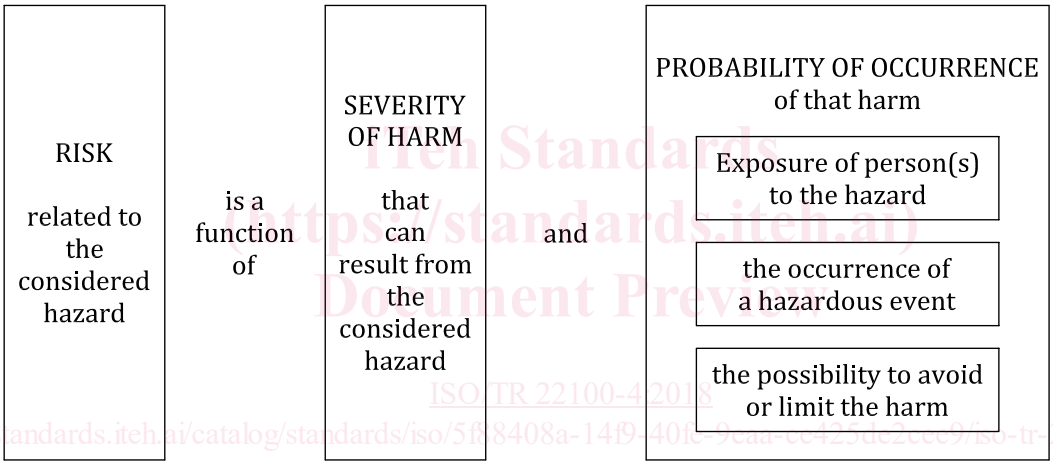

Figure 1 — Elements of risk related to safety of machinery (see ISO 12100:2010, Figure 3)

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

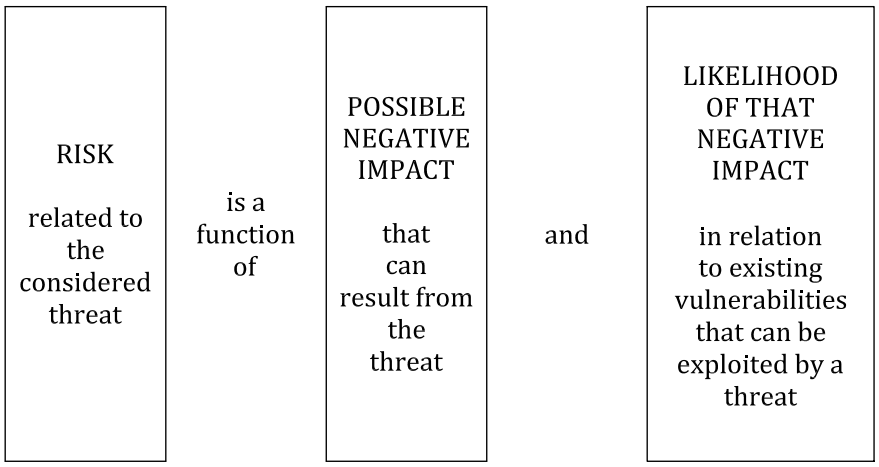

Figure 2 — Elements of risk related to IT-security