



DPC: 24/30490377 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 13 December 2024

Origin: European

Latest date for receipt of comments: 05 February 2025

Project No. 2024/00975

Responsible committee: MCE/3 Safeguarding of machinery

Interested committees:

Title: Draft BS EN ISO 12100 Safety of machinery - General principles for design - Risk assessment and risk reduction.

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 05 February 2025

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

Responsible Committee Secretary: Mr Christopher Brown (BSI)
Direct tel: 02089967441
E-mail: christopher.brown@bsigroup.com

Full document details: 24/30490377 DC

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



DRAFT International Standard

ISO/DIS 12100

Safety of machinery — General principles for design — Risk assessment and risk reduction

*Sécurité des machines — Principes généraux de conception —
Appréciation du risque et réduction du risque*

ICS: 13.110

ISO/TC 199

Secretariat: **DIN**

Voting begins on:
2024-12-13

Voting terminates on:
2025-03-07

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

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.

Reference number
ISO/DIS 12100:2024(en)

Full document details: 24/30490377 DC

© ISO 2024  **Documents**
Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO 2024

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
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Strategy for risk assessment and risk reduction	9
5 Risk assessment	14
5.1 General	14
5.2 Information for risk assessment	15
5.3 Determination of limits of machinery	16
5.3.1 General	16
5.3.2 Use limits	16
5.3.3 Space limits	16
5.3.4 Time limits	17
5.3.5 Other limits	17
5.4 Hazard identification	17
5.5 Risk estimation	19
5.5.1 General	19
5.5.2 Elements of risk	19
5.5.3 Aspects to be considered during risk estimation	21
5.6 Risk evaluation	23
5.6.1 General	23
5.6.2 Adequate risk reduction	23
5.6.3 Comparison of risks	23
6 Risk reduction	24
6.1 General	24
6.2 Inherently safe design	24
6.2.1 General	24
6.2.2 Consideration of geometrical factors and physical aspects	25
6.2.3 Taking into account general technical knowledge of machine design	26
6.2.4 Choice of appropriate technology	26
6.2.5 Applying principle of positive mechanical action	27
6.2.6 Provisions for stability	27
6.2.7 Provisions for maintainability	27
6.2.8 Observing ergonomics principles	28
6.2.9 Electrical hazards	29
6.2.10 Pneumatic and hydraulic hazards	29
6.2.11 Limiting exposure to hazards through reliability of equipment	29
6.2.12 Limiting exposure to hazards through mechanization or automation of loading (feeding) / unloading (removal) operations	29
6.2.13 Limiting exposure to hazards through location of setting and maintenance points outside danger zones	30
6.2.14 Hygiene aspects	30
6.3 Safeguarding and complementary risk reduction measures	30
6.3.1 General	30
6.3.2 Selection and implementation of guards and protective devices	30
6.3.3 Requirements for design of guards and protective devices	31
6.3.4 Safeguarding to reduce emissions	34
6.3.5 Design of control systems	34
6.3.6 Complementary risk reduction measures	41
6.4 Information for use	43
6.4.1 General requirements	43
6.4.2 Location and nature of information for use	43

ISO/DIS 12100:2024(en)

6.4.3	Signals and warning devices	44
6.4.4	Markings, signs (pictograms) and written warnings	44
6.4.5	Accompanying documents (in particular — instruction handbook)	45
7	Documentation of risk assessment and risk reduction	47
Annex A	(informative) Schematic representation of a machine	49
Annex B	(informative) Examples of hazards, hazardous situations and hazardous events	50
Annex C	(informative) Using the system of type-A, type-B and type-C standards to design a machine to achieve a level of tolerable risk by adequate risk reduction	61
Annex D	(informative) How this document relates to ISO 13849-1	65
Annex E	(informative) Trilingual lookup and index of specific terms and expressions used in this document	70
Annex ZA	(informative) Relationship between this European Standard and the essential requirements of Directive 2006/42/EC aimed to be covered	83
Annex ZB	(informative) Relationship between this European Standard and the essential requirements of Regulation (EU) 2023/1230 aimed to be covered	84
Annex ZC	(informative) Relation of this document to the Machinery Directive 2006/42/EC	85
Annex ZD	(informative) Relation of this document to the Regulation (EU) 2023/1230	86
Bibliography		87

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.

This second edition cancels and replaces the first edition (ISO 12100:2010) which has been technically revised as well as ISO/TR 22100-1:2021 and ISO/TR 22100-2:2013, the technical content of which have been incorporated.

The main changes are as follows:

- new second paragraph and new Note 3 added to Scope;
- ISO 20607, IEC 61508-3 and IEC 62061 additionally referenced normatively;
- terms and definitions: “*relevant hazard*” (former 3.7), “*failure to danger*” (former 3.32) and “*comparative emission data*” (former 3.42) deleted; “*tolerable risk*” and “*cybersecurity*” added; term “*risk reduction measure*” introduced to replace deprecated term “*protective measure*” and definition of “*risk evaluation*” adjusted to ISO/IEC Guide 51;
- new [Figure 1](#) additionally added;
- requirements for control systems moved to [6.3.6](#);
- reference to evolving behaviour of applied artificial intelligence added to [5.4](#), b) 2);
- [Figure 4](#) replaced by new [Figure 5](#);
- new subclause “Hygiene aspects” added as [6.2.14](#);
- subclause “Safeguarding to reduce emissions” shortened on general aspects only;
- subclause on “Software aspects” completely rewritten;
- new subclause “Cybersecurity and protection against corruption” added as [6.3.5.15](#);
- ISO/TR 22100-1 and ISO/TR 22100-2 incorporated as new [Annexes C](#) and [D](#).

Introduction

The primary purpose of this document is to provide designers with an overall framework and guidance for decisions during the development of machinery to enable them to design machines that are adequately safe for their intended use. It also provides a strategy for standards developers and will assist in the preparation of consistent and appropriate type-B and type-C standards.

The concept of safety of machinery considers the ability of a machine to perform its intended function(s) during its life cycle where risk has been adequately reduced.

This document is the basis for a set of standards which has the following structure:

- a) **type-A standards** (basic safety standards) giving basic concepts, principles for design, and general aspects that can be applied to all machinery;
- b) **type-B standards** (generic safety standards) dealing with one safety aspect or one or more type(s) of safeguard that can be used across a wide range of machinery:
 - type-B1 standards on particular safety aspects (e.g., safety distances, surface temperature, noise);
 - type-B2 standards on safeguards (e.g., two-hand control devices, interlocking devices, pressure-sensitive devices, guards);
- c) **type-C standards** (machine safety standards) dealing with detailed safety requirements for a particular machine or group of machines.

This document is a type-A standard.

This document is of relevance, in particular, for the following stakeholder groups representing the market players with regard to machinery safety:

- machine manufacturers (small, medium and large enterprises);
- health and safety bodies (regulators, accident prevention organisations, market surveillance);

Others can be affected by the level of machinery safety achieved with the means of the document by the above-mentioned stakeholder groups:

- machine users/employers (small, medium and large enterprises);
- machine users/employees (e.g. trade unions, organizations for people with special needs);
- service providers, e.g. for maintenance (small, medium and large enterprises);
- consumers (in case of machinery intended for use by consumers).

The above-mentioned stakeholder groups have been given the possibility to participate in the drafting process of this document.

When a type-C standard deviates from one or more technical provisions dealt with by this document or by a type-B standard, the type-C standard takes precedence.

It is desirable that this document be referred to in training courses and manuals to convey basic terminology and general design methods to designers.

ISO/IEC Guide 51 has been taken into account as far as practicable at the time of drafting of this document.

Safety of machinery — General principles for design — Risk assessment and risk reduction

1 Scope

This document specifies basic terminology, principles and a methodology for achieving safety in the design of machinery. It specifies principles of risk assessment and risk reduction to help designers in achieving this objective. These principles are based on knowledge and experience of the design, use, incidents, accidents and risks associated with machinery. Procedures are described for identifying hazards and estimating and evaluating risks during relevant phases of the machine life cycle, and for the elimination of hazards or the provision of adequate risk reduction. Guidance is given on the documentation and verification of the risk assessment and risk reduction process.

This document covers principal implications on machinery safety in case of implementation of artificial intelligence/machine learning, and vulnerability against cybersecurity attacks / corruption regarding their impact on safety. It specifies generic measures to address both aspects.

Safety of machinery includes hygiene aspects.

This document is also intended to be used as a basis for the preparation of type-B or type-C safety standards.

It does not cover risk and/or damage to domestic animals, property or the environment.

NOTE 1 While this document refers to risks of harm to persons, the risk assessment process set out in this document can be equally effective in assessing other types of risks such as damage to domestic animals, property or the environment.

NOTE 2 [Annex B](#) gives, in separate tables, examples of hazards, hazardous situations and hazardous events, in order to clarify these concepts and assist the designer in the process of hazard identification.

NOTE 3 The practical use of a number of methods for each stage of risk assessment is described in ISO/TR 14121-2.

NOTE 4 As used in this document the designer of a machine can include the manufacturer, integrator, supplier; or the user in case of safety-relevant modifications.

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 20607, *Safety of machinery — Instruction handbook — General drafting principles*

IEC 60204-1:2021¹⁾, *Safety of machinery — Electrical equipment of machines — Part 1: General requirements*

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

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

1) i.e. Edition 6.1 which combines IEC 60204-1:2016 and Amendment 1, AMD 1:2021.

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1 machinery

machine

an assembly, fitted with or intended to be fitted with a drive system other than directly applied human or animal effort, consisting of linked parts or components, at least one of which moves, and which are joined together for a specific application

Note 1 to entry: The term “machinery” also covers an assembly of machines which, in order to achieve the same end, are arranged and controlled so that they function as an integral whole.

Note 2 to entry: [Annex A](#) provides a general schematic representation of a machine.

3.2 reliability

ability of a machine or its components or equipment to perform a required function under specified conditions and for a given period of time without failing

3.3 maintainability

ability of a machine to be maintained in a state which enables it to fulfil its function under conditions of intended use, or to be restored to such a state

3.4 usability

ability of a machine to be easily used including properties or characteristics that enable its function(s) to be easily understood

3.5 harm

physical injury or damage to health

3.6 hazard

potential source of harm

Note 1 to entry: The term “hazard” can be qualified in order to define its origin (for example, mechanical hazard, electrical hazard) or the nature of the potential harm (for example, electric shock hazard, cutting hazard, toxic hazard, fire hazard).

Note 2 to entry: The hazard envisaged by this definition either

- is permanently present during the intended use of the machine (for example, motion of hazardous moving elements, electric arc during a welding phase, unhealthy posture, noise emission, high temperature), or
- can appear unexpectedly (for example, explosion, crushing hazard as a consequence of an unintended/unexpected start-up, ejection as a consequence of a breakage, fall as a consequence of acceleration/deceleration).

3.7 significant hazard

hazard which has been identified as associated with the machine and which requires specific action by the designer to eliminate or to reduce the risk according to the risk assessment

Note 1 to entry: This term is included as basic terminology for type-B and type-C standards.

Note 2 to entry: The deprecated term 'relevant' is included as being a significant hazard.

**3.8
hazardous event**

event that can cause harm

Note 1 to entry: A hazardous event can occur over a short period of time or over an extended period of time.

**3.9
hazardous situation**

circumstance in which a person is exposed to at least one hazard

Note 1 to entry: The exposure can result in harm immediately or over a period of time.

**3.10
hazard zone**

danger zone

any space within and/or around machinery in which a person can be exposed to a hazard

**3.11
risk**

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

**3.12
residual risk**

risk remaining after risk reduction measures have been implemented

Note 1 to entry: This document distinguishes

- the residual risk after risk reduction measures have been implemented by the designer,
- the residual risk remaining after all risk reduction measures by the designer and the user have been implemented.

Note 2 to entry: See also [Figure 3](#).

**3.13
risk estimation**

defining likely severity of harm and probability of its occurrence

**3.14
risk analysis**

combination of the specification of the limits of the machine, hazard identification and risk estimation

**3.15
risk evaluation**

procedure based on the risk analysis to determine whether further risk reduction is required

[SOURCE: ISO/IEC Guide 51:2014, definition 3.12, modified – The wording “tolerable risk has been exceeded” has been replaced with “further risk reduction required”.]

**3.16
risk assessment**

overall process comprising a risk analysis and a risk evaluation

Note 1 to entry: See [Figure 1](#).

**3.17
adequate risk reduction**

risk reduction that is at least in accordance with legal requirements, taking into consideration the current state of the art

Note 1 to entry: Criteria for determining when adequate risk reduction is achieved are given in [5.6.2](#).

3.18

risk reduction measure

DEPRECATED: protective measure

action or means to eliminate hazards or reduce risks

Note 1 to entry: See [Figure 2](#).

3.19

tolerable risk

acceptable risk

level of risk that is accepted in a given context based on the current values of society

Note 1 to entry: Tolerable risk usually refers to the level at which further technologically, functionally and financially feasible risk reduction measures or additional expenditure(s) of resources will not result in significant reduction in risk.

Note 2 to entry: A similar phrase used in some ISO standards is *“the risk has been adequately reduced”*.

3.20

inherently safe design

risk reduction measure which either eliminates hazards or reduces the risks associated with hazards by changing the design or operating characteristics of the machine without the use of guards or protective devices

Note 1 to entry: See [6.2](#).

3.21

safeguarding

risk reduction measure using safeguards to protect persons from the hazards which cannot reasonably be eliminated or risks which cannot be sufficiently reduced by inherently safe design

Note 1 to entry: See [6.3](#).

3.22

information for use

risk reduction measure consisting of communication links (for example, text, words, signs, signals, symbols, diagrams) used separately or in combination, to convey information to the user

Note 1 to entry: See [6.4](#).

3.23

intended use

use of a machine in accordance with the information for use

3.24

reasonably foreseeable misuse

use of a machine in a way not intended by the designer, but which can result from readily predictable human behaviour

3.25

task

specific activity performed by one or more persons on, or in the vicinity of, the machine during its life cycle

3.26

safeguard

guard or protective device

3.27

guard

physical barrier, designed as part of the machine to provide protection

Note 1 to entry: A guard may act either

- alone, in which case it is only effective when “closed” (for a movable guard) or “securely held in place” (for a fixed guard), or

- in conjunction with an interlocking device with or without guard locking, in which case protection is ensured whatever the position of the guard.

Note 2 to entry: Depending on its construction, a guard may be described as, for example, casing, shield, cover, screen, door, enclosing guard.

Note 3 to entry: The terms for types of guards are defined in [3.27.1](#) to [3.27.6](#). See also [6.3.3.2](#) and ISO 14120 for types of guards and their requirements.

3.27.1

fixed guard

guard affixed in such a manner (for example, by screws, nuts, welding) that it can only be opened or removed by the use of tools or by destruction of the affixing means

3.27.2

movable guard

guard which can be opened without the use of tools

3.27.3

adjustable guard

fixed or movable guard which is adjustable as a whole or which incorporates adjustable part(s)

3.27.4

interlocking guard

guard associated with an interlocking device such that, together with the control system of the machine, prevents the:

- operation of the hazardous machine functions associated with the guard until the guard is closed,
- and if the guard is opened while hazardous machine functions are operating, a command to bring the machine to a safe (a stop command) is given,

Note 1 to entry: An interlocking guard can contain/be equipped with one or more interlocking devices. These interlocking devices can also be of different types.

Note 2 to entry: The generation of the (stop) command to bring the machine to a safe state when the guard is open does not apply to guards locked with a trapped key interlocking system.

Note 3 to entry: ISO 14119 gives detailed provisions.

3.27.5

interlocking guard with guard locking

guard associated with an interlocking device and a guard locking device so that, together with the control system of the machine, the following functions are performed:

- the hazardous machine functions associated with the guard cannot operate until the guard is closed and locked,
- the guard remains closed and locked until the risk due to the hazardous machine functions associated with the guard has ceased, and
- when the guard is closed and locked, the hazardous machine functions associated with the guard can operate (the closure and locking of the guard do not by themselves start the hazardous machine functions)

Note 1 to entry: ISO 14119 gives detailed provisions.

3.27.6

interlocking guard with a start function

control guard

special form of interlocking guard which, once it has reached its closed position, gives a command to initiate the hazardous machine function(s) without the use of a separate start control

Note 1 to entry: See [6.3.3.2.5](#) for detailed provisions on the conditions of use.

3.28

protective device

safeguard other than a guard

Note 1 to entry: Examples of types of protective devices are [3.28.1](#) to [3.28.8](#).

3.28.1

interlocking device

interlock

mechanical, electrical or other type of device, the purpose of which is to prevent the operation of hazardous machine functions under specified conditions (generally as long as a guard is not closed)

3.28.2

enabling device

additional manually operated device used in conjunction with a start control and which, when continuously actuated, allows a machine to function

3.28.3

hold-to-run control device

control device which initiates and maintains machine functions only as long as the manual control (actuator) is actuated

3.28.4

two-hand control device

control device which requires simultaneous actuation by both hands in order to initiate and to maintain hazardous machine functions, thus providing a risk reduction measure only for the person who actuates it

Note 1 to entry: ISO 13851 gives detailed provisions.

3.28.5

sensitive protective equipment

SPE

equipment for detecting persons or parts of persons which generates an appropriate signal to the control system to reduce risk to the persons detected

Note 1 to entry: The signal can be generated when a person or part of a person goes beyond a predetermined limit, for example, enters a hazard zone (tripping) or when a person is detected in a predetermined zone (presence sensing), or in both cases.

3.28.6

active optoelectronic protective device

AOPD

device whose sensing function is performed by optoelectronic emitting and receiving elements detecting the interruption of optical radiation, generated within the device, by an opaque object present in the specified detection zone

Note 1 to entry: The IEC 61496 series gives detailed provisions.

3.28.7

limiting device

device which prevents a machine or hazardous machine condition(s) from exceeding a designed limit (space limit, pressure limit, load moment limit, speed limit etc.)

3.28.8

mechanical restraint device

device which introduces into a mechanism a mechanical obstacle (for example, wedge, spindle, strut, slide locks, safety blocks, scotch (pin)) which by virtue of its own span, can prevent any hazardous movement

3.28.9

limited movement control device

control device, a single actuation of which, together with the control system of the machine, permits only a limited amount of travel of a machine element

3.29

impeding device

any physical obstacle (low barrier, rail, etc.) which, without totally preventing access to a hazard zone, reduces the probability of access to this zone by offering an obstruction to free access

3.30

safety function

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

3.31

unexpected start-up

unintended start-up

any start-up which, because of its unexpected nature, generates a risk to persons

Note 1 to entry: For example, this can be caused by

- a start command which is the result of a failure in or an external influence on the control system,
- a start command generated by inopportune action on a start control or other parts of the machine such as a sensor or a power control element,
- restoration of the power supply after an interruption,
- external/internal influences (gravity, wind, self-ignition in internal combustion engines, etc.) on parts of the machine.

Note 2 to entry: Machine start-up during normal sequence of an automatic cycle is not *unintended*, but can be considered as being *unexpected* from the point of view of the operator. Prevention of hazardous situations in this case involves the use of safeguarding measures (see [6.3](#)).

[SOURCE: ISO 14118:2017, definition 3.2, modified – The word “any” has been added at the begin of the definition. In the second sentence of Note 2 to entry “hazardous events” has been replaced by “hazardous situations”.]

3.32

fault (of an item)

inability to perform as required, due to an internal state

Note 1 to entry: A fault of an item results from a failure, either of the item itself, or from a deficiency in an earlier stage of the life cycle, such as specification, design, manufacture or maintenance. See latent fault (192-04-08).

Note 2 to entry: Qualifiers, such as specification, design, manufacture, maintenance or misuse, may be used to indicate the cause of a fault.

Note 3 to entry: The type of fault may be associated with the type of associated failure, e.g. wear-out fault and wear-out failure.

Note 4 to entry: The adjective “faulty” designates an item having one or more faults.

[SOURCE: IEC 60050-192:2015, 192-04-01]

3.33

failure

failure (of an item)

loss of ability to perform as required

Note 1 to entry: A failure of an item is an event that results in a fault of that item: see fault (192-04-01).

Note 2 to entry: Qualifiers, such as catastrophic, critical, major, minor, marginal and insignificant, may be used to categorize failures according to the severity of consequences, the choice and definitions of severity criteria depending upon the field of application.

Note 3 to entry: Qualifiers, such as misuse, mishandling and weakness, may be used to categorize failures according to the cause of failure.

[SOURCE: IEC 60050-192:2015, 192-03-01]

3.34

common cause failures

failures of multiple items, which would otherwise be considered independent of one another, resulting from a single cause

Note 1 to entry: Common cause failures can also be common mode failures (192-03-19).

Note 2 to entry: The potential for common cause failures reduces the effectiveness of system redundancy.

[SOURCE: IEC 60050-192:2015, 192-03-18]

3.35

common mode failures

common mode failures (within a system), pl

failures of different items characterized by the same failure mode

Note 1 to entry: Common mode failures may have different causes.

Note 2 to entry: Common mode failures can also be common cause failures (192-03-18).

Note 3 to entry: The potential for common mode failures reduces the effectiveness of system redundancy.

[SOURCE: IEC 60050-192:2015, 192-03-19]

3.36

malfunction

failure of a machine to perform an intended function

Note 1 to entry: See [5.4](#), item b) 2) for examples.

3.37

emergency situation

hazardous situation needing to be urgently ended or averted

Note 1 to entry: An emergency situation can arise

- during normal operation of the machine (for example, due to human interaction, or as a result of external influences), or
- as a consequence of a malfunction or failure of any part of the machine.

3.38

emergency operation

all actions and functions intended to end or avert an emergency situation

3.39

emergency stop

emergency stop function

function which is intended to

- avert arising or reduce existing hazards to persons, damage to machinery or to work in progress, and
- be initiated by a single human action

Note 1 to entry: ISO 13850 gives detailed provisions.

3.40

emission value

numerical value quantifying an emission generated by a machine (for example, noise, vibration, hazardous substances, radiation)

Note 1 to entry: Emission values are part of the information on the properties of a machine and are used as a basis for risk assessment.

Note 2 to entry: The term “*emission value*” ought not to be confused with “*exposure value*”, which quantifies the exposure of persons to emissions when the machine is in use. Exposure values can be estimated using the emission values.

Note 3 to entry: Emission values are preferably measured and their associated uncertainties determined by means of standardized methods (for example, to allow comparison between similar machines).

3.41

cybersecurity

measures to protect a machine control system against unauthorized access or attack that can result in a hazardous situation

Note 1 to entry: Damage or changes can be made to the machine control system hardware, software or information, as well as from disruption or misdirection of the intended function

Note 2 to entry: Cybersecurity is covering both, information technology security (IT security) and operational technology (OT). See also ISO 23806.

4 Strategy for risk assessment and risk reduction

To implement risk assessment and risk reduction, the following actions shall be taken, in the order given (see [Figure 1](#) and [Figure 2](#)):

Determine the limits of the machinery, which include the intended use and any reasonably foreseeable misuse thereof

NOTE 1 Any misuse of a machine which is illegal or not readily predictable human behaviour is outside the scope of a risk assessment. However, cybersecurity attacks with potential impacts to safety should be considered.

- a) identify the hazards and associated hazardous situations;
- b) estimate the risk for each identified hazard and hazardous situation;
- c) evaluate the risk and make decisions about the need for risk reduction;
- d) eliminate the hazard or reduce the risk associated with the hazard by means of risk reduction measures until the risk is adequately reduced to achieve tolerable risk.

Actions a) to d) are related to risk assessment, and e) to risk reduction.

[Figure 1](#) shows the overall approach to the risk assessment/risk reduction process.

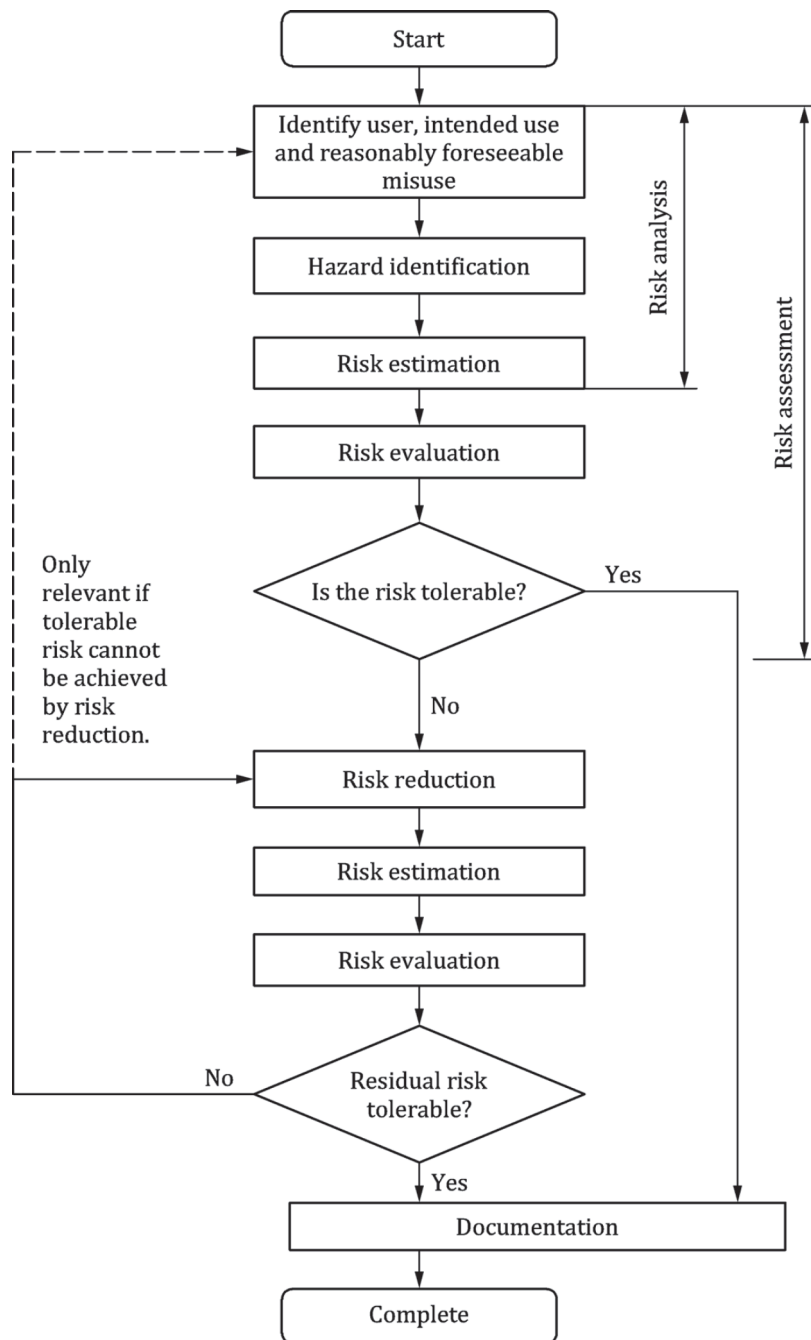


Figure 1 — Iterative process of risk assessment and risk reduction [see ISO/IEC Guide 51:2014]

Two important aspects of the overall process in [Figure 1](#) are

- identifying hazards, hazardous situations and hazardous events, and
- reducing risks.

Resources and efforts should be focused on these two key elements. Nevertheless, other aspects of the process shown in [Figure 1](#) are necessary and important.

Risk assessment is a series of logical steps to enable, in a systematic way, the analysis and evaluation of the risks associated with machinery.

Risk assessment is followed, whenever necessary, by risk reduction. Iteration of this process can be necessary to eliminate hazards as far as practicable and to adequately reduce risks by the implementation of risk reduction measures.

Note 2 It is generally accepted that the residual risk is equal or lower than the tolerable risk.

The method to implement the process of [Figure 1](#) is shown in [Figure 2](#). [Figure 2](#) intentionally mirrors [Figure 1](#), but provides additional details on the aspects of the three steps of risk reduction to be taken by the machine designer to achieve tolerable risk. Whereas [Figure 1](#) highlights the “what” of the risk assessment process, [Figure 2](#) demonstrates “how” the intended risk reduction is achieved.

NOTE 3 This document deals only with the application of risk reduction measures by the designer.

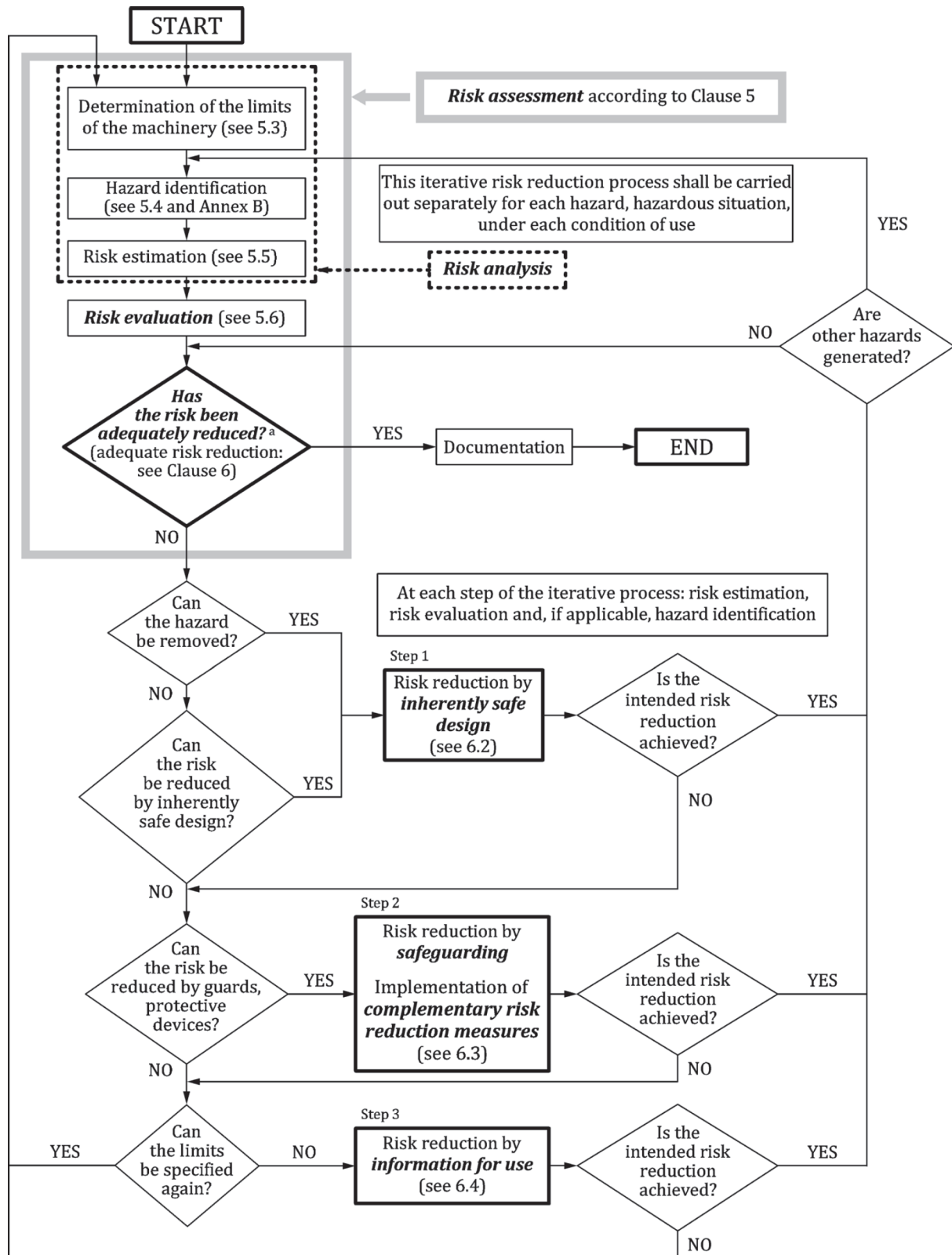
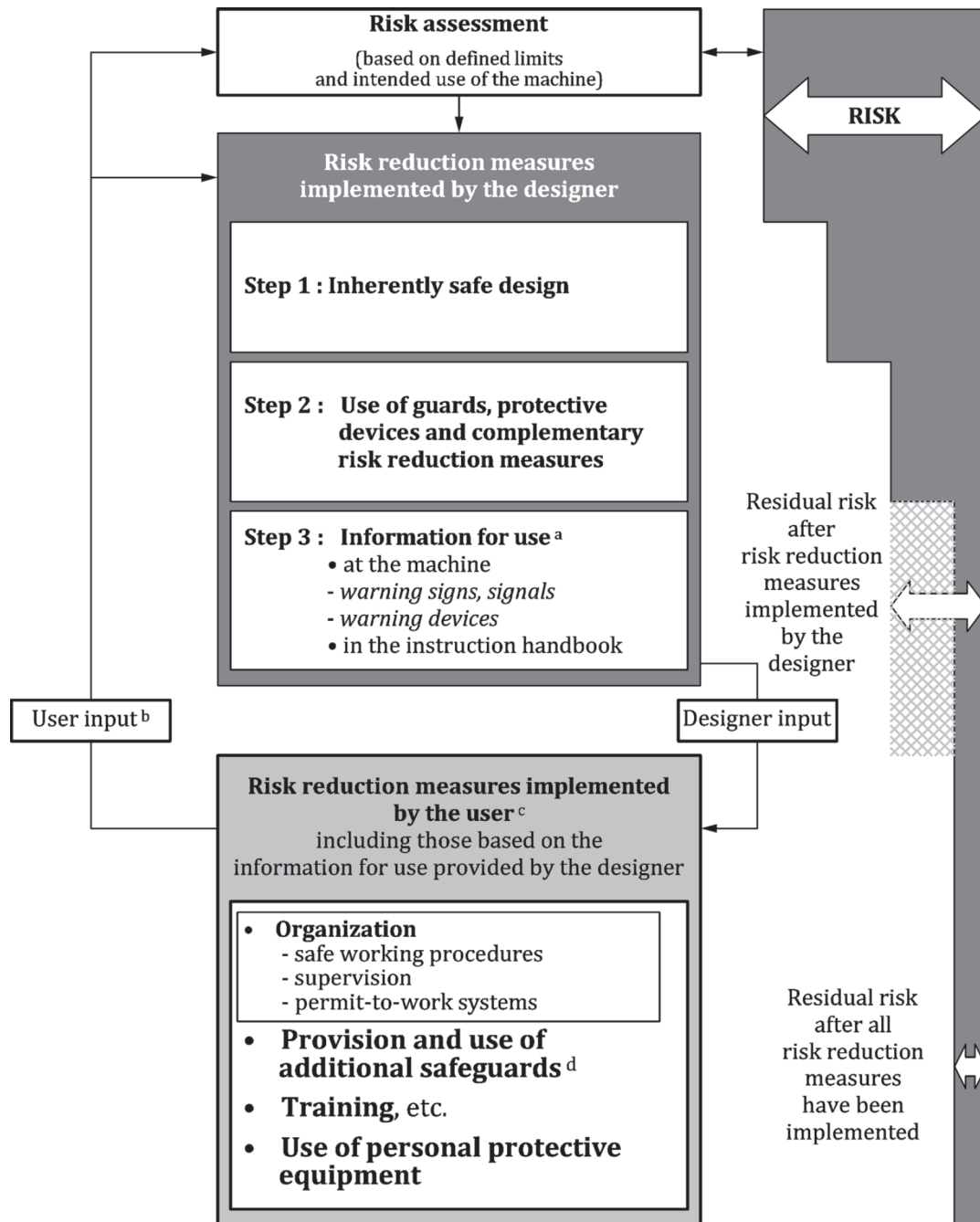


Figure 2 — Schematic representation of risk reduction process including iterative three-step method

Risk reduction measures are the combination of the measures implemented by the designer and the user in accordance with [Figure 3](#). Measures which can be incorporated at the design stage are preferable to those implemented by the user and usually prove more effective.

Further details on the impact of risk reduction measures taken by both the machine designer and machine user are shown in [Figure 3](#). The impacts shown illustrate the effectiveness of the three-step method shown in [Figure 2](#) and the information flow between the designer and user in order to achieve and maintain an overall outcome of tolerable risk.



- ^a Providing proper information for use is part of the designer's contribution to risk reduction, but the risk reduction measures concerned are only effective when implemented by the user.
- ^b The user input is that information received by the designer from either the user community, regarding the intended use of the machine in general, or from a specific user.
- ^c These risk reduction measures are outside the scope of this document.
- ^d These are risk reduction measures required due to a specific process or processes not envisaged in the intended use of the machine or to specific conditions for installation that cannot be controlled by the designer.

Figure 3 — Risk reduction process from point of view of designer

The objective to be met is the greatest practicable risk reduction, taking into account the four factors below. The strategy defined in this Clause is represented by the flowcharts in [Figure 1](#) and [Figure 2](#). The process itself is iterative and several successive applications can be necessary to reduce the risk, making the best use of available technology. In carrying out this process, it is necessary to take into account these four factors, in the following order of preference:

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

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

NOTE 5 A machine design which is acceptable at a particular time could be no longer justifiable when technological development allows the design of an equivalent machine with lower risk.

As result of this process it shall be assumed that the particular machine will result in a design that can be used with tolerable risk achieved by adequate risk reduction (see [Figure 1](#)).

[Annex C](#) provides guidance as to how the system of existing type-A, type-B and type-C standards on machinery safety should be applied in order to design a machine to achieve a level of tolerable risk by adequate risk reduction. It explains how this type-A standard should be used for practical cases in conjunction with type-B and type-C standards on machinery safety.

All products and systems include hazards and, therefore, some level of residual risk. However, the risk associated with those hazards shall be reduced to a tolerable level.

5 Risk assessment

5.1 General

Risk assessment (see [Figure 2](#)) comprises

- risk analysis, comprising
 - a) determination of the limits of the machinery (see [5.3](#)),
 - b) hazard identification (see [5.4](#) and [Annex B](#)), and
 - c) risk estimation (see [5.5](#)), and
- risk evaluation (see [5.6](#)).

Risk analysis provides information required for the risk evaluation, which in turn allows judgments to be made about whether or not risk reduction is required.

These judgments shall be supported by a qualitative or, where appropriate, quantitative estimate of the risk associated with the hazards present on the machinery.

NOTE A quantitative approach can be appropriate when useful data are available. However, a quantitative approach is restricted by the useful data that are available and/or the limited resources of those conducting the risk assessment. Therefore, in many applications only qualitative risk estimation will be possible.

The risk assessment shall be documented according to [Clause 7](#).

5.2 Information for risk assessment

5.2.1 The information for risk assessment should include the following.

a) **Related to machinery description:**

- 1) user input and specifications;
- 2) anticipated machinery specifications, including
 - i) a description of the various phases of the whole life cycle of the machinery,
 - ii) design drawings or other means of establishing the nature of the machinery, and
 - iii) required energy sources and how they are supplied;
- 3) documentation on previous designs of similar machinery, if relevant;
- 4) information for use of the machinery, as available.

b) **Related to regulations, standards and other applicable documents:**

- 1) applicable regulations;
- 2) relevant standards;
- 3) relevant technical specifications;
- 4) relevant safety data sheets.

c) **Related to experience of use:**

- 1) any accident, incident or malfunction history of the actual or similar machinery;
- 2) the history of damage to health resulting, for example, from emissions (noise, vibration, dust, fumes, etc.), chemicals used or materials processed by the machinery;
- 3) the experience of users of similar machines and, whenever practicable, an exchange of information with the potential users.

NOTE An incident that has occurred and resulted in harm can be referred to as an “accident”, whereas an incident that has occurred and that did not result in harm can be referred to as a “near miss”.

d) **Related to human factors and ergonomics aspects, e.g.:**

- 1) required variability for different operators; e.g. size, weight, maneuverability
- 2) required work postures or movements and manual force exertions;
- 3) required space for movements of the parts of the operator's body;
- 4) required human-machine interactions;
- 5) machine work rate.

5.2.2 The information shall be updated as the design develops or when modifications to the machine are required.

Comparisons between similar hazardous situations associated with different types of machinery are often possible, provided that sufficient information about hazards and accident circumstances in those situations is available.

NOTE The absence of an accident history, a small number of accidents or low severity of accidents ought not to be taken as a presumption of a low risk.

For quantitative analysis, data from databases, handbooks, laboratories or manufacturers' specifications may be used, provided that there is confidence in the suitability of the data. Uncertainty associated with these data shall be indicated in the documentation (see [Clause 7](#)).

5.3 Determination of limits of machinery

5.3.1 General

Risk assessment begins with the determination of the limits of the machinery, taking into account all the phases of the machinery life. This means that the characteristics and performances of the machine or a series of machines in an integrated process, and the related people, environment and products, should be identified in terms of the limits of machinery as given in [5.3.2](#) to [5.3.5](#).

5.3.2 Use limits

Use limits include the intended use and the reasonably foreseeable misuse. Aspects to be taken into account include the following:

- a) the machine operating modes and intervention procedures for the users, including interventions required by malfunctions of the machine;
- b) the use of the machinery (for example, industrial, non-industrial and domestic) by persons identified by sex, dominant hand usage, age, or limiting physical abilities (visual or hearing impairment, size, strength, etc.);
- c) the anticipated levels of training, experience or ability of users including
 - 1) operators,
 - 2) maintenance personnel or technicians,
 - 3) trainees and apprentices, and
 - 4) the general public;
- d) exposure of other persons to the hazards associated with the machinery where it can be reasonably foreseen:
 - 1) persons likely to have a good awareness of the specific hazards, such as operators of adjacent machinery;
 - 2) persons with little awareness of the specific hazards but likely to have a good awareness of site safety procedures, authorized routes, etc., such as administration staff;
 - 3) persons likely to have very little awareness of the machine hazards or the site safety procedures, such as visitors or members of the general public, including children.

If specific information is not available in relation to b), above, the manufacturer should take into account general information on the intended user population (for example, appropriate anthropometric data).

- e) specific limitations of cybersecurity attributes for a machine
- f) limitations for the use of artificial intelligence (e.g. machine learning), such as the type of data used to train artificial intelligence system.

5.3.3 Space limits

Aspects of space limits to be taken into account include

- a) the range of movement,
- b) space requirements for persons interacting with the machine, such as during operation and maintenance,

- c) human interaction such as the operator-machine interface, and
- d) the machine-power supply interface.

5.3.4 Time limits

Aspects of time limits to be taken into account include

- a) the life limit of the machinery and/or of some of its components (tooling, parts that can wear, electromechanical components, etc.), taking into account its intended use and reasonably foreseeable misuse, and
- b) recommended service intervals.

5.3.5 Other limits

Examples of other limits include

- a) properties of the material(s) to be processed,
- b) housekeeping — the level of cleanliness required, and
- c) environmental — the recommended minimum and maximum temperatures, whether the machine can be operated indoors or outdoors, in dry or wet weather, in direct sunlight, tolerance to dust and wet, etc.

5.4 Hazard identification

After determination of the limits of the machinery, the essential step in any risk assessment of the machinery is the systematic identification of reasonably foreseeable hazards (permanent hazards and those which can appear unexpectedly), hazardous situations and/or hazardous events during all phases of the machine life cycle, i.e.:

- transport, assembly and installation;
- commissioning;
- use;
- dismantling, disabling and scrapping.

Only when hazards have been identified can steps be taken to eliminate them or to reduce risks. To accomplish this hazard identification, it is necessary to identify the operations to be performed by the machinery and the tasks to be performed by persons who interact with it, taking into account the different parts, mechanisms or functions of the machine, the materials to be processed, if any, and the environment in which the machine can be used.

The designer shall identify hazards taking into account the following.

a) Human interaction with machinery during the life cycle of the machine

Task identification shall be performed for all modes of operation and all tasks associated with every phase of the machine life cycle as given above. Task identification shall also take into account, but not be limited to, the following tasks:

- setting;
- testing;
- teaching/programming;
- process/tool changeover;
- starting the machine;

- feeding the machine;
- removal of product from machine;
- stopping the machine;
- stopping the machine in case of emergency;
- recovery of operation from jam or blockage;
- restart after unscheduled stop;
- fault-finding/trouble-shooting (operator intervention);
- cleaning and housekeeping;
- preventive maintenance;
- corrective maintenance.

All reasonably foreseeable hazards, hazardous situations or hazardous events associated with the various tasks shall then be identified. [Annex B](#) gives examples of hazards, hazardous situations and hazardous events to assist in this process. Several methods are available for the systematic identification of hazards. See also ISO/TR 14121-2.

In addition, reasonably foreseeable hazards, hazardous situations or hazardous events not directly related to tasks shall be identified.

EXAMPLE Seismic events, lightning, excessive snow loads, noise, break-up of machinery, hydraulic hose burst.

b) Possible states of the machine

These are as follows:

- 1) the machine performs the intended function (the machine operates normally);
- 2) the machine does not perform the intended function (i.e. malfunctions) due to a variety of reasons, including
 - variation of a property or of a dimension of the processed material or of the workpiece,
 - failure of one or more of its component parts or services,
 - external disturbances (for example, shocks, vibration, electromagnetic interference),
 - design error or deficiency (for example, software errors),
 - disturbance of its power supply, and
 - surrounding conditions (for example, damaged floor surfaces)
 - unintended self evolving behaviour of applied artificial intelligence (see ISO/TR 22100-5)
 - cybersecurity breach

NOTE 1 At the design stage, the machine manufacturer should observe basic principles/measures to minimize the cybersecurity risks of safety-related parts of the entire machine (see [6.3.5.7.3](#)).

NOTE 2 A cybersecurity breach does not introduce new hazards however it should be seen as a source for initiating hazardous events e.g., cyber is an additional consideration. See also ISO/TR 22100-4.

c) Unintended behaviour of the operator or reasonably foreseeable misuse of the machine

Examples include

- loss of control of the machine by the operator (especially for hand-held or mobile machines),

- reflex behaviour of a person in case of malfunction, incident or failure during the use of the machine,
- behaviour resulting from lack of concentration or carelessness,
- behaviour resulting from taking the “line of least resistance” in carrying out a task,
- behaviour resulting from pressures to keep the machine running in all circumstances, and
- behaviour of certain persons (for example, children, disabled persons).

NOTE Examination of the available design documentation can be a useful means of identifying hazards related to the machinery, particularly those associated with moving elements such as motors or hydraulic cylinders.

5.5 Risk estimation

5.5.1 General

After hazard identification, risk estimation shall be carried out for each hazardous situation by determining the elements of risk given in [5.5.2](#). When determining these elements, it is necessary to take into account the aspects given in [5.5.3](#).

5.5.2 Elements of risk

5.5.2.1 General

The risk associated with a particular hazardous situation depends on the following elements:

- a) the severity of harm;
- b) the probability of occurrence of that harm, which is a function of
 - 1) the exposure of person(s) to the hazard,
 - 2) the occurrence of a hazardous event, and
 - 3) the technical and human possibilities to avoid or limit the harm.

The elements of risk are shown in [Figure 4](#). Additional details are given in [5.5.2.2](#), [5.5.2.3](#) and [5.5.3](#).

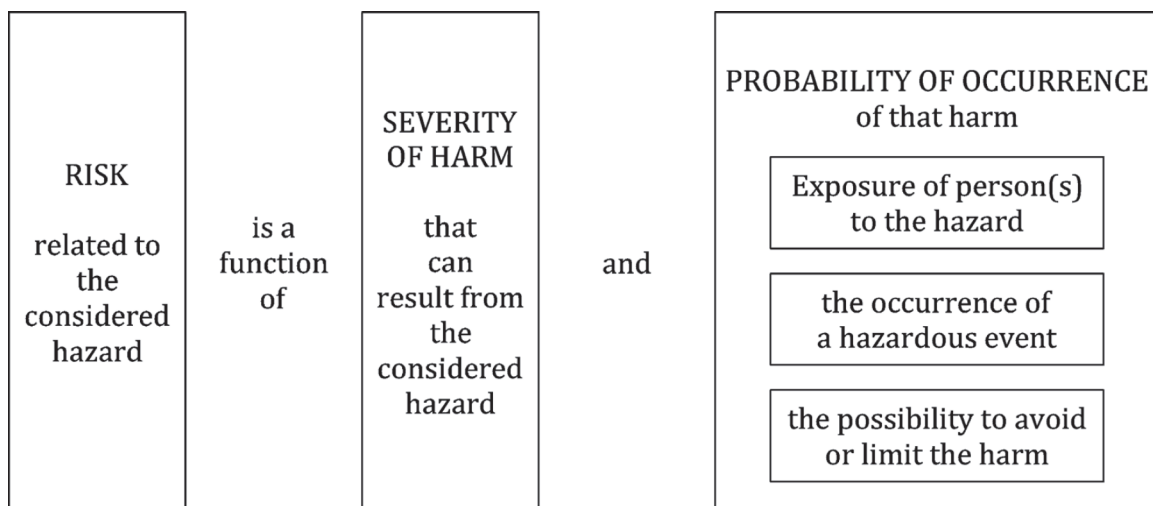


Figure 4 — Elements of risk

5.5.2.2 Severity of harm

The severity can be estimated by taking into account the following:

- a) the severity of injuries or damage to health, for example,
 - slight,
 - serious,
 - death.
- b) the extent of harm, for example, to
 - one person,
 - several persons due to a single hazardous event.

When carrying out a risk assessment, the risk from the most severe harm that can realistically occur from each identified hazard, even if the probability of such an occurrence is not high, shall be considered. See ISO/TR 14121-2.

5.5.2.3 Probability of occurrence of harm

5.5.2.3.1 Exposure of persons to the hazard

The exposure of a person to the hazard influences the probability of the occurrence of harm. Factors to be taken into account when estimating the exposure are, among others,

- a) the need for access to the hazard zone, e.g. during use, correction of malfunction, maintenance, repair,
- b) the nature of access (e.g., manual feeding of materials),
- c) the time spent in the hazard zone,
- d) the number of persons requiring access, and
- e) the frequency of access.

5.5.2.3.2 Occurrence of a hazardous event

The occurrence of a hazardous event influences the probability of occurrence of harm. Factors to be taken into account when estimating the occurrence of a hazardous event are, among others,

- a) reliability and other statistical data,
- b) accident history,
- c) history of damage to health, and
- d) comparison of risks (see [5.6.3](#)).

NOTE The occurrence of a hazardous event can be of a technical or human origin.

5.5.2.4 Possibility of avoiding or limiting harm

The possibility of avoiding or limiting harm influences the probability of occurrence of harm. Factors to be taken into account when estimating the possibility of avoiding or limiting harm are, among others, the following:

- a) different persons who can be exposed to the hazard(s), for example,
 - skilled,

- unskilled;
- b) how quickly the hazardous situation could lead to harm, for example,
 - suddenly,
 - quickly,
 - slowly;
- c) any awareness of risk, for example,
 - by general information,
 - by direct observation,
 - through warning signs and indicating devices, in particular, on the machinery;
- d) the human ability to avoid or limit harm (for example, reflex, agility, possibility of escape);
- e) practical experience and knowledge, for example,
 - of the machinery,
 - of similar machinery,
 - no experience.

5.5.3 Aspects to be considered during risk estimation

5.5.3.1 Persons exposed

Risk estimation shall take into account all persons (operators and others) for whom exposure to the hazard is reasonably foreseeable.

5.5.3.2 Type, frequency and duration of exposure

The estimation of the exposure to the hazard under consideration (including long-term damage to health) requires analysis of, and shall account for, all modes of operation of the machinery and methods of working. In particular, the analysis shall account for the needs for access during loading/unloading, setting, teaching, process changeover or correction, cleaning, fault-finding and maintenance.

The risk estimation shall also take into account tasks, for which it is necessary to suspend risk reduction measures.

5.5.3.3 Relationship between exposure and effects

The relationship between an exposure to a hazard and its effects shall be taken into account for each hazardous situation considered. The effects of accumulated exposure and combinations of hazards shall also be considered. When considering these effects, risk estimation shall, as far as practicable, be based on appropriate recognized data.

NOTE 1 Accident data can assist in establishing the probability and severity of injury associated with the use of a particular type of machinery with a particular type of risk reduction measure.

NOTE 2 Zero accident data is, however, no guarantee of the low probability and severity of an injury.

5.5.3.4 Human factors and ergonomics

Human factors can affect risk and shall be taken into account in the risk estimation, including, for example,

- a) the interaction of person(s) with the machinery, including correction of malfunction,

- b) interaction between persons,
- c) stress-related aspects,
- d) ergonomics aspects,
- e) the capacity of persons to be aware of risks in a given situation depending on their training, experience and ability,
- f) fatigue aspects, and
- g) aspects of limited abilities (due to disability, age, etc.).

Training, experience and ability can affect risk; nevertheless, none of these factors shall be used as a substitute for hazard elimination, risk reduction by inherently safe design or safeguarding, wherever these risk reduction measures can be practicably implemented.

5.5.3.5 Suitability of risk reduction measures

Risk estimation shall take into account the suitability of risk reduction measures and shall

- a) identify the circumstances which can result in harm,
- b) whenever appropriate, be carried out using quantitative methods to compare alternative risk reduction measures (see ISO/TR 14121-2), and
- c) provide information that can assist with the selection of appropriate risk reduction measures.

When estimating risk, those components and systems identified as immediately increasing the risk in case of failure need special attention.

When risk reduction measures include user organization measures, competency requirements or correct behaviour, attention, use of personal protective equipment (PPE), skill or training, the relatively low reliability of such risk reduction measures compared with proven technical risk reduction measures shall be taken into account by the designer in the risk estimation.

5.5.3.6 Possibility of defeating or circumventing risk reduction measures

For the continued safe operation of a machine, it is important that the risk reduction measures allow its easy use and do not hinder its intended use. Otherwise, there is a possibility that risk reduction measures might be bypassed in order for maximum utility of the machine to be achieved.

Risk estimation shall take account of the possibility of defeating or circumventing risk reduction measures. It shall also take account of the incentive to defeat or circumvent risk reduction measures when, for example,

- a) the risk reduction measure slows down production or interferes with another activity or preference of the user,
- b) the risk reduction measure is difficult to use,
- c) persons other than the operator are involved, or
- d) the risk reduction measure is not recognized by the user or not accepted as being suitable for its function,
- e) the risk reduction measure prevents a task or operation from being performed.

Whether or not a risk reduction measure can be defeated depends on both the type of risk reduction measure, such as an adjustable guard or programmable trip device, and its design details.

Risk reduction measures that use programmable electronic control systems introduce additional possibilities of defeat or circumvention if access to safety-related software is not appropriately restricted by design and monitoring methods. Risk estimation shall identify where safety-related functions are not