INTERNATIONAL STANDARD

ISO 12100

First edition
2010-11-01

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

Reference number
ISO 12100:2010(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO 12100 was prepared by Technical Committee ISO/TC 199, *Safety of machinery*.

This first edition of ISO 12100 cancels and replaces ISO 12100-1:2003, ISO 12100-2:2003 and ISO 14121-1:2007, of which it constitutes a consolidation without technical change. It also incorporates the Amendments ISO 12100-1:2003/Amd.1:2009 and ISO 12100-2:2003/Amd.1:2009. Documentation (e.g. risk assessment, type-C standards) based on these replaced documents need not be updated or revised.

Introduction

The primary purpose of this International Standard 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 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 International Standard is the basis for a set of standards which has the following structure:

— **type-A standards** (basic safety standards) giving basic concepts, principles for design and general aspects that can be applied to machinery;

— **type-B standards** (generic safety standards) dealing with one safety aspect or one type of safeguard that can be used across a wide range of machinery:

  — type-B1 standards on particular safety aspects (for example, safety distances, surface temperature, noise);

  — type-B2 standards on safeguards (for example, two-hand controls, interlocking devices, pressure-sensitive devices, guards);

— **type-C standards** (machine safety standards) dealing with detailed safety requirements for a particular machine or group of machines.

This International Standard is a type-A standard.

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

It is desirable that this International Standard 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 International Standard.

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

1 Scope

This International Standard 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 sufficient risk reduction. Guidance is given on the documentation and verification of the risk assessment and risk reduction process.

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

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

NOTE 1 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 2 The practical use of a number of methods for each stage of risk assessment is described in ISO/TR 14121-2.

2 Normative references

The following referenced documents are indispensable for the application 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.

IEC 60204-1:2005, *Safety of machinery — Electrical equipment of machines — Part 1: General requirements*

3 Terms and definitions

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

3.1
machinery
machine
assembly, fitted with or intended to be fitted with a drive system consisting of linked parts or components, at least one of which moves, and which are joined together for a specific application

NOTE 1 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 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, with the necessary actions (maintenance) being carried out according to specified practices and using specified means

3.4
usability
ability of a machine to be easily used owing to, among others, 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 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 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).

NOTE 3 The French term "*phénomène dangereux*" should not be confused with the term "*risque*", which was sometimes used instead in the past.

3.7
relevant hazard
hazard which is identified as being present at, or associated with, the machine

NOTE 1 A relevant hazard is identified as the result of one step of the process described in Clause 5.

NOTE 2 This term is included as basic terminology for type-B and type-C standards.

3.8
significant hazard
hazard which has been identified as relevant and which requires specific action by the designer to eliminate or to reduce the risk according to the risk assessment

NOTE This term is included as basic terminology for type-B and type-C standards.

3.9
hazardous event
event that can cause harm

NOTE A hazardous event can occur over a short period of time or over an extended period of time.

3.10
hazardous situation
circumstance in which a person is exposed to at least one hazard

NOTE The exposure can result in harm immediately or over a period of time.

3.11
hazard zone
danger zone
any space within and/or around machinery in which a person can be exposed to a hazard

3.12
risk
combination of the probability of occurrence of harm and the severity of that harm

3.13
residual risk
risk remaining after protective measures have been implemented

NOTE 1 This International Standard distinguishes

— the residual risk after protective measures have been implemented by the designer,

— the residual risk remaining after all protective measures have been implemented.

NOTE 2 See also Figure 2.

3.14
risk estimation
defining likely severity of harm and probability of its occurrence

3.15
risk analysis
combination of the specification of the limits of the machine, hazard identification and risk estimation

3.16
risk evaluation
judgment, on the basis of risk analysis, of whether the risk reduction objectives have been achieved

3.17
risk assessment
overall process comprising a risk analysis and a risk evaluation

3.18
adequate risk reduction
risk reduction that is at least in accordance with legal requirements, taking into consideration the current state of the art

NOTE Criteria for determining when adequate risk reduction is achieved are given in 5.6.2.

3.19
protective measure
measure intended to achieve risk reduction, implemented

— by the designer (inherently safe design, safeguarding and complementary protective measures, information for use) and/or

— by the user (organization: safe working procedures, supervision, permit-to-work systems; provision and use of additional safeguards; use of personal protective equipment; training)

NOTE See Figure 2.

3.20
inherently safe design measure
protective 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 See 6.2.

3.21
safeguarding
protective 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 measures

NOTE See 6.3.

3.22
information for use
protective 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 See 6.4.

3.23
intended use
use of a machine in accordance with the information for use provided in the instructions

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

NOTE 3 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 so that, together with the control system of the machine, the following functions are performed:

— the hazardous machine functions "covered" by the guard cannot operate until the guard is closed,

— if the guard is opened while hazardous machine functions are operating, a stop command is given, and

— when the guard is closed, the hazardous machine functions "covered" by the guard can operate (the closure of the guard does not by itself start the hazardous machine functions)

NOTE 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 "covered" by 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 "covered" by the guard has disappeared, and

— when the guard is closed and locked, the hazardous machine functions "covered" by the guard can operate (the closure and locking of the guard do not by themselves start the hazardous machine functions)

NOTE 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 See 6.3.3.2.5 for detailed provisions on the conditions of use.

3.28
protective device
safeguard other than a guard

NOTE Examples of types of protective devices are 3.28.1 to 3.28.9.

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 at least simultaneous actuation by both hands in order to initiate and to maintain hazardous machine functions, thus providing a protective measure only for the person who actuates it

NOTE 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 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 IEC 61496 gives detailed provisions.

3.28.7
mechanical restraint device
device which introduces into a mechanism a mechanical obstacle (for example, wedge, spindle, strut, scotch) which, by virtue of its own strength, can prevent any hazardous movement

3.28.8
limiting device
device which prevents a machine or hazardous machine condition(s) from exceeding a designed limit (space limit, pressure limit, load moment limit, etc.)

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 This can be caused by, for example:

— 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 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 accidents in this case involves the use of safeguarding measures (see 6.3).

NOTE 3 Adapted from ISO 14118:2000, definition 3.2.

3.32
failure to danger
any malfunction in the machinery, or in its power supply, that increases the risk

3.33
fault
state of an item characterized by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources

[IEV 191-05-01]

NOTE 1 A fault is often the result of a failure of the item itself, but can exist without prior failure.

NOTE 2 In the field of machinery, the English term “fault” is commonly used in accordance with the definition in IEV 191-05-01, whereas the French term “*défaut*” and the German term “*Fehler*” are used rather than the terms “*panne*” and “*Fehlzustand*” that appear in the IEV with this definition.

NOTE 3 In practice, the terms “fault” and “failure” are often used synonymously.

3.34
failure
termination of the ability of an item to perform a required function

NOTE 1 After failure, the item has a fault.

NOTE 2 “Failure” is an event, as distinguished from “fault”, which is a state.

NOTE 3 The concept as defined does not apply to items consisting of software only.

[IEV 191-04-01]

3.35
common cause failures
failures of different items, resulting from a single event, where these failures are not consequences of each other

NOTE Common cause failures should not be confused with common mode failures.

[IEV 191-04-23]

3.36
common mode failures
failures of items characterized by the same fault mode

NOTE Common mode failures should not be confused with common cause failures, as the common mode failures can result from different causes.

[IEV 191-04-24]

3.37
malfunction
failure of a machine to perform an intended function

NOTE See 5.4, item b) 2) for examples.

3.38
emergency situation
hazardous situation needing to be urgently ended or averted

NOTE 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.

3.39
emergency operation
all actions and functions intended to end or avert an emergency situation

3.40
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 ISO 13850 gives detailed provisions.

3.41
emission value
numerical value quantifying an emission generated by a machine (for example, noise, vibration, hazardous substances, radiation)

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

NOTE 2 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 Emission values are preferably measured and their associated uncertainties determined by means of standardized methods (for example, to allow comparison between similar machines).

3.42
comparative emission data
set of emission values of similar machines collected for the purpose of comparison

NOTE For noise comparison, see ISO 11689.

4 Strategy for risk assessment and risk reduction

To implement risk assessment and risk reduction the designer shall take the following actions, in the order given (see Figure 1):

a) determine the limits of the machinery, which include the intended use and any reasonably foreseeable misuse thereof;

b) identify the hazards and associated hazardous situations;

c) estimate the risk for each identified hazard and hazardous situation;

d) evaluate the risk and take decisions about the need for risk reduction;

e) eliminate the hazard or reduce the risk associated with the hazard by means of protective measures.

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

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 protective measures.

It is assumed that, when present on machinery, a hazard will sooner or later lead to harm if no protective measure or measures have been implemented. Examples of hazards are given in Annex B.

Protective measures are the combination of the measures implemented by the designer and the user in accordance with Figure 2. Measures which can be incorporated at the design stage are preferable to those implemented by the user and usually prove more effective.

The objective to be met is the greatest practicable risk reduction, taking into account the four below factors. The strategy defined in this clause is represented by the flowchart in Figure 1. 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 1 The ideal application of these principles requires knowledge of the 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 2 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.