ISO 13849-1:2023

Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design

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,* in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/TC 114, *Safety of machinery,* in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This fourth edition cancels and replaces the third edition (ISO 13849-1:2015), which has been technically revised.

The main changes are as follows:

- - the whole document was reorganized to better follow the design and development process for control systems;
- - new Clause 4 on recommendation for risk assessment;
- - specification of the safety functions (updated Clause 5);
- - combination of several subsystems (updated in Clause 6);
- - new Clause 7 on software safety requirements;
- - new Clause 9 on ergonomic aspects of design;
- - validation (updated Clause 8 and moved to Clause 10);
- - new G.5 on management of the functional safety;

- - new Annex L on electromagnetic interference (EMI) immunity;
- - new Annex M with additional information for safety requirements specification;
- - new Annex N on fault-avoiding measures for the design of safety related software;
- - new Annex O with safety-related values of components or parts of the control systems.

A list of all parts in the ISO 13849 series can be found on the ISO website.
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.

Introduction
The structure of safety standards in the field of machinery is as follows:

- a) Type-A standards (basis standards) give basic concepts, principles for design and general aspects that can be applied to machinery.
- b) Type-B standards (generic safety standards) deal with one or more safety aspect(s), or one or more type(s) of safeguards 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 controls, interlocking devices, pressure sensitive devices, guards).
- c) Type-C standards (machinery safety standards) deal with detailed safety requirements for a particular machine or group of machines.

This document is a type-B1 standard as defined in ISO 12100:2010.
The first edition of this document was published in 1999 based on EN 954-1:1996 (withdrawn standard). The second edition was revised in 2006 and the third edition was revised in 2015.

This document is of relevance, in particular for the following stakeholder groups 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:

- - machine users/employers (small, medium and large enterprises);
- - machine users/employees (e.g. trade unions);
- - service providers, e.g. for maintenance (small, medium and large enterprises);
- - consumers (i.e. 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.
In addition, this document is intended for standardization bodies elaborating type-C standards, as defined in ISO 12100:2010.

The requirements of this document can be supplemented or modified by a type-C standard.

For machines which are covered by the scope of a type-C standard and which have been designed and built according to the requirements of that standard, the requirements of that type-C standard take precedence.

NOTE 1 The examples and basis for most content is based on stationary machines in factory applications. However, other machines are not excluded. This document was written without considering if certain machinery (e.g. mobile machinery) has specific requirements. However, this document is intended to be used across many machinery industries and as a basis for type-C standards developers, as far as applicable.

This document is intended to give guidance to those involved in the design and assessment of control systems, and those preparing type-B2 or type-C standards.

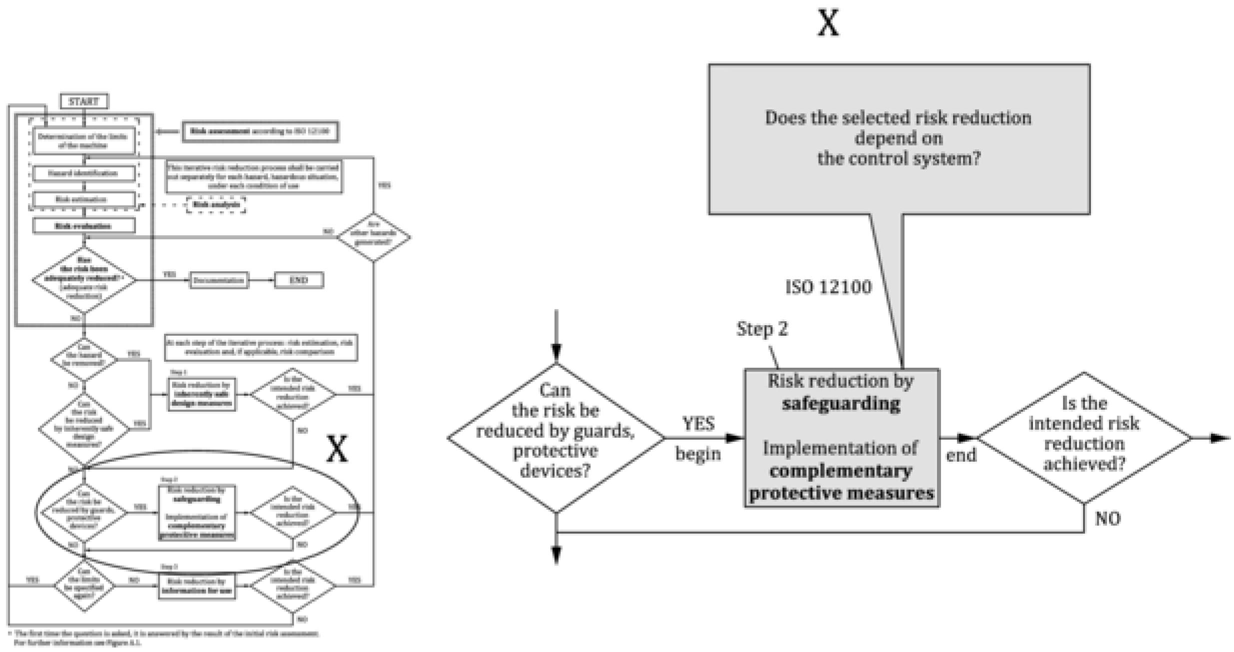
Risk reduction according to ISO 12100:2010, Clause 6, is accomplished by applying, in the following sequence, inherently safe design measures, safeguarding and/or complementary risk reduction measures and information for use. A designer can reduce risks by risk reduction measures that can have safety functions. Parts of machinery control systems that are assigned to provide safety functions are called safety-related parts of control systems (SRP/CS). These can consist of hardware or a combination of hardware and software and can either be separate from the machine control system or an integral part of it. In addition to implementing safety functions, SRP/CS can also implement operational functions.

ISO 12100:2010 is used for risk assessment of the machine. Annex A of this document can be used for the determination of the required performance level (PL_r) of a safety function performed by the SRP/CS, where its PL_r is not specified in the applicable type-C standard. This document is relevant for the SRP/CS safety functions that are used to address risks for cases where a risk assessment conducted according to ISO 12100:2010 determines that a risk reduction measure is needed that relies on a safety function (e.g. interlocking guard). In those cases, the safety-related control system performs a safety function. This document is intended to be used to design and evaluate the SRP/CS. Only the part of the control system that is safety-related falls under the scope of this document.

Figure 1 illustrates the relationship between ISO 12100:2010 and this document. For a detailed overview see Figure 2.

NOTE 2 See also ISO/TR 22100-2:2013 for further information.

Figure 1 - Integration of this document (ISO 13849-1) within the risk reduction process of ISO 12100:2010



NOTE Based on ISO/TR 22100-2:2013, Figure 2.

NOTE 3 Figure 1 shows where the SRP/CS contributes to the risk reduction process of ISO 12100:2010: Step 2. The SRP/CS supports the combined risk reduction measures by the implementation of safety functions. The ability of safety-related parts of control systems to perform a safety function under foreseeable conditions is allocated one of five levels, called performance levels (PL). The required performance level (PL_r) for a particular safety function (depending on the required risk reduction) will be determined by risk estimation.

Informative Annex A of this document contains a method for risk estimation and can be used for the determination of the PL_r of a safety function performed by the SRP/CS. Any risk estimation method will show a variance because of the subjective nature of the evaluation criteria. In comparison to Annex A, type-C standards can have more specific risk estimation methods for specific machine applications.

The frequency of dangerous failure of the safety function depends on several factors, including but not limited to, hardware and software structure, the extent of fault detection mechanisms [diagnostic coverage (DC)], reliability of components [mean time to dangerous failure ($MTTF_D$), common cause failure (CCF)], design process, operating stress, environmental conditions and operation procedures.

In order to facilitate the design of SRP/CS and the assessment of achieved PL, this document employs a methodology based on the categorization of architectures with specific design criteria (e.g. $MTTF_D$, DC_{avg}) and specified behaviour under fault conditions. These architectures are allocated one of five levels termed Categories B, 1, 2, 3 and 4.

Functional safety considers the failure characteristics of elements/components performing a safety function. For each safety function, this failure characteristic is expressed as the frequency of dangerous failure per hour (PFH).

The performance levels and categories can be applied to SRP/CS, e.g.:

- - control units (e.g. a logic unit for control functions, data processing, monitoring);
- - electro-sensitive protective devices (e.g. photoelectric barriers), pressure sensitive devices.

The performance levels can be defined, and categories determined, for subsystems of SRP/CS using safety parts (components), e.g.:

- - protective devices (e.g. two-hand control devices, interlocking devices);
- - power control elements (e.g. relays, valves);
- - sensors and HMI elements (e.g. position sensors, enable switches).

Machinery covered by this document can range from simple (e.g. small kitchen machines, or automatic doors and gates) to complex (e.g. packaging machines, printing machines, presses and integrated machinery into a system).
This document and IEC 62061 both specify a methodology and provide related guidance for the design and implementation of safety-related control systems of machinery.

The requirements of Clause 10 of this document supersede the requirements of ISO 13849-2:2012 (excluding the informative annexes).

1 Scope

This document specifies a methodology and provides related requirements, recommendations and guidance for the design and integration of safety-related parts of control systems (SRP/CS) that perform safety functions, including the design of software.

This document applies to SRP/CS for high demand and continuous modes of operation including their subsystems, regardless of the type of technology and energy (e.g. electrical, hydraulic, pneumatic, and mechanical). This document does not apply to low demand mode of operation.

NOTE 1 See 3.1.44 and the IEC 61508 series for low demand mode of operation.

This document does not specify the safety functions or required performance levels (PL_r) that are to be used in particular applications.

NOTE 2 This document specifies a methodology for SRP/CS design without considering if certain machinery (e.g. mobile machinery) has specific requirements. These specific requirements can be considered in a Type-C standard.

This document does not give specific requirements for the design of products/components that are parts of SRP/CS. Specific requirements for the design of some components of SRP/CS are covered by applicable ISO and IEC standards.

This document does not provide specific measures for security aspects (e.g. physical, IT-security, cyber security).

NOTE 3 Security issues can have an effect on safety functions. See ISO/TR 22100-4 and IEC/TR 63074 for further information.

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*
- ISO 13849-2:2012, *Safety of machinery - Safety-related parts of control systems - Part 2: Validation*
- ISO 13855:2010, *Safety of machinery - Positioning of safeguards with respect to the approach speeds of parts of the human body*
- ISO 20607:2019, *Safety of machinery - Instruction handbook - General drafting principles*
- IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements*
- IEC 62046:2018, *Safety of machinery - Application of protective equipment to detect the presence of persons*
- IEC 62061:2021, *Safety of machinery - Functional safety of safety-related control systems*
- IEC/IEEE 82079-1:2019, *Preparation of information for use (instructions for use) of products - Part 1: Principles and general requirements*

3 Terms, definitions, symbols and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 12100:2010 and the following apply.

ISO and IEC maintain terminology 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/

3.1.1
safety-related part of a control system

SRP/CS

part of a control system that performs a **safety function** (3.1.27), starting from a safety-related input(s) to generating a safety-related output(s)

Note 1 to entry: The safety-related parts of a control system start at the point where the safety-related inputs are initiated (including, for example, the actuating cam and the roller of the position switch) and end at the output of the power control elements (including, for example, the main contacts of a contactor).

3.1.2

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 and mechanical).

3.1.3

safety requirements specification

SRS

specification containing the requirements for the **safety functions** (3.1.27) that have to be met by the safety-related control system in terms of characteristics of the safety functions (functional requirements) and **required performance levels (PL_r)** (3.1.6)

[SOURCE:IEC 61508-4:2010, 3.5.11, modified - Information from IEC 61508-4:2010, 3.5.12 has been included.]

3.1.4

category

classification of the **subsystem** (3.1.45) in respect to its resistance to **faults** (3.1.8) and the subsequent behaviour in the fault condition which is achieved by the structural arrangement of the parts, fault detection and/or by their reliability

3.1.5

performance level

PL

discrete level used to specify the ability of *safety-related parts of control systems* **(SRP/CS)** (3.1.1) to perform a **safety function** (3.1.27) under foreseeable conditions

Note 1 to entry: See 6.1 for a general overview of performance level.

3.1.6

required performance level

PL_r

performance level (3.1.5) required in order to achieve the required **risk** (3.1.19) reduction for each **safety function** (3.1.27)

Note 1 to entry: See 5.3 and Figure A.1 for further information on required performance level (PL_r).

3.1.7

safety integrity level

SIL

discrete level (one out of a possible four) for specifying the safety integrity requirements of **safety functions** (3.1.27) to be allocated to the safety-related systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

Note 1 to entry: In this document only SIL 1 to SIL 3 are considered.

[SOURCE:IEC 61508-4:2010, 3.5.8, modified - "allocated to safety-related systems" has been added to definition, NOTES have been deleted and new Note 1 to entry has been added.]

3.1.8

fault

abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function

Note 1 to entry: A fault is often the result of a **failure** (3.1.10) of the item itself, but can exist without prior failure.

Note 2 to entry: In this document "fault" means random fault or fault caused by a **systematic failure** (3.1.14).

[SOURCE:IEC 60050-192:2015, modified - Note 2 to entry has been amended.]

3.1.9

fault exclusion

exclusion of certain **faults** (3.1.8) within a safety-related part of a control system (SRP/CS), if this exclusion can be justified due to the negligible probability of these faults

3.1.10

failure

termination of the ability of a device to perform a required function

Note 1 to entry: After a failure, the device has a **fault** (3.1.8).

Note 2 to entry: "Failure" is an event, as distinguished from "fault", which is a state.

Note 3 to entry: Failures which only affect the availability of the process under control are outside of the scope of this document.

[SOURCE:IEC 60050-192:2015, modified - Note 3 to entry has been amended.]

3.1.11

permanent fault

fault (3.1.8) of an item that persists until an action of corrective maintenance is performed

[SOURCE:IEC 60050-192:2015]

3.1.12

dangerous failure

failure (3.1.10) of an element and/or **subsystem** (3.1.45) and/or system that plays a part in implementing the **safety function** (3.1.27) that:

- a) prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the machine/machinery is put into a hazardous or potentially hazardous state; or
- b) decreases the probability that the safety function operates correctly when required

[SOURCE:IEC 61508-4:2010, 3.6.7, modified - "EUC" has been replaced by "machine/machinery".]

3.1.13

common cause failure

CCF

failure (3.1.10) that is the result of one or more events, causing concurrent failures of two or more separate **channels** (3.1.47) in a multiple channel **subsystem** (3.1.45), leading to failure of a **safety function** (3.1.27)

Note 1 to entry: Common cause failures are not identical with common mode failures (see ISO 12100:2010, 3.36).

[SOURCE:IEC 61508-4:2010, 3.6.10, modified - "system failure" has been changed to "failure of a safety function". Note 1 to entry has been added.]

3.1.14

systematic failure

failure (3.1.10) related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

Note 1 to entry: Corrective maintenance without modification will usually not eliminate the failure cause.

Note 2 to entry: A systematic failure can be induced by simulating the failure cause.

Note 3 to entry: Examples of causes of systematic failures include human error in

- - the *safety requirements specification* **(SRS)** (3.1.3),
- - the design, manufacture, installation, operation of the hardware,
- - the design, implementation, of the software, and
- - inadequately specifying environmental conditions.

[SOURCE:IEC 60050-192:2015]

3.1.15

muting

temporary automatic suspension of a **safety function(s)** (3.1.27) by the SRP/CS

[SOURCE:IEC 61496-1:2020, 3.16]

3.1.16

harm

physical injury or damage to health

[SOURCE:ISO 12100:2010, 3.5]

3.1.17

hazard

potential source of **harm** (3.1.16)

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

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

- - is permanently present during the intended use of the machine (e.g. motion of hazardous moving elements, electric arc during a welding phase, unhealthy posture, noise emission, high temperature); or
- - can appear unexpectedly (e.g. 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).

[SOURCE:ISO 12100:2010, 3.6, modified - Note 3 to entry has been deleted.]

3.1.18

hazardous situation

circumstance in which a person is exposed to at least one **hazard** (3.1.17)

Note 1 to entry: The exposure can result in **harm** (3.1.16) immediately or over a period of time.

[SOURCE:ISO 12100:2010, 3.10]

3.1.19

risk

combination of the probability of occurrence of **harm** (3.1.16) and the severity of that harm

[SOURCE:ISO 12100:2010, 3.12]

3.1.20

residual risk

risk (3.1.19) remaining after *risk reduction measures* **(protective measures)** (3.1.22) have been taken

Note 1 to entry: See Figure 3.

[SOURCE:ISO 12100:2010, 3.13, modified - Note 1 to entry has been modified.]

3.1.21

risk assessment

overall process comprising **risk analysis** (3.1.23) and **risk evaluation** (3.1.24)

[SOURCE:ISO 12100:2010, 3.17]

3.1.22

risk reduction measure

protective measure

action or means to eliminate **hazards** (3.1.17) or reduce **risks** (3.1.19)

EXAMPLE:

Inherently safe design; protective devices; personal protective equipment; information for use and installation; organization of work; training; application of equipment; supervision.

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

3.1.23

risk analysis

combination of the specification of the limits of the machine, **hazard** (3.1.17) identification and **risk** (3.1.19) estimation

[SOURCE:ISO 12100:2010, 3.15]

3.1.24

risk evaluation

judgement, on the basis of **risk analysis** (3.1.23), of whether risk reduction objectives have been achieved

[SOURCE:ISO 12100:2010, 3.16]

3.1.25

intended use of the machine

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

[SOURCE:ISO 12100:2010, 3.23]

3.1.26

reasonably foreseeable misuse

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

[SOURCE:ISO 12100:2010, 3.24]

3.1.27

safety function

function of a machine whose **failure** (3.1.10) can result in an immediate increase of the **risk(s)** (3.1.19)

Note 1 to entry: A safety function is a function implemented by a safety-related part of a control system, which is needed to achieve or maintain a safe state for the machine, in respect of a specific hazardous event.

[SOURCE:ISO 12100:2010, 3.30, modified - Note 1 to entry has been added.]

3.1.28

sub-function

part of a **safety function** (3.1.27) whose **failure** (3.1.10) results in a failure of the safety function

Note 1 to entry: A sub-function is a function implemented by a **subsystem** (3.1.45) of the safety-related part of a control system (SRP/CS). See also IEC 61800-5-2:2016.

EXAMPLE:

Sub-functions according to IEC 61800-5-2 are, e.g. safe torque off (STO), safe stop 1 (SS1). See Figure 6.

3.1.29

monitoring

diagnostic measure which detects a state and compares it to the expected value

Note 1 to entry: Monitoring is realised by the following methods, e.g. **plausibility check** (3.1.52), direct, indirect or **cross monitoring** (3.1.30) (see Annex E), cyclic test stimulus.

3.1.30

cross monitoring

diagnostic measure which checks plausibility of redundant signals in both **channels** (3.1.47) of a redundant **subsystem** (3.1.45)

3.1.31

programmable electronic system

PE system

system for control, protection or **monitoring** (3.1.29) based on one or more programmable electronic devices, including all elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, and actuators and other output devices

[SOURCE:IEC 61508-4:2010, 3.3.1]

3.1.32

mean time to dangerous failure

$MTTF_D$

expectation of the mean time to dangerous failure

Note 1 to entry: In the case of items with an exponential distribution of operating times to dangerous failure (i.e. a constant failure rate) the $MTTF_D$ is numerically equal to the reciprocal of the dangerous failure rate.

[SOURCE:IEC 62061:2021, 3.2.38, modified - Note 1 to entry has been modified.]

3.1.33

MTBF

mean time between failures

expected value of the operating time between consecutive **failures** (3.1.10)

3.1.34

RDF

ratio of dangerous failures

fraction of the overall **failure** (3.1.10) rate of an element that can result in a **dangerous failure** (3.1.12)

3.1.35

diagnostic coverage

DC

measure of the effectiveness of diagnostics, which is determined as the ratio between the **failure** (3.1.10) rate of detected **dangerous failures** (3.1.12) and the failure rate of total dangerous failures

Note 1 to entry: Diagnostic coverage can exist for the whole or parts of a safety-related system. For example, diagnostic coverage can exist for sensors and/or logic systems and/or power control elements.

3.1.36

mission time

T_M

period of time covering the intended use of a safety-related part of a control system (SRP/CS)

3.1.37

test rate

r_t

frequency of tests to detect **faults** (3.1.8) in a safety-related part of a control system (SRP/CS)

Note 1 to entry: Test rate is also used as reciprocal value of diagnostic test interval.

3.1.38

demand rate

r_d

frequency of demands for a **safety function** (3.1.27) to be performed by the safety-related part of a control system (SRP/CS)

3.1.39

limited variability language

LVL

type of language that provides the capability to combine predefined, application specific, library functions to implement the *safety requirements specifications* **(SRSs)** (3.1.3)

Note 1 to entry: An LVL provides a close functional correspondence with the functions required to achieve the application.

Note 2 to entry: Typical examples of LVL are given in IEC 61131-3. They include ladder diagram, function block diagram and sequential function chart. Instruction lists and structured text are not considered to be LVL.

Note 3 to entry: Typical example of systems using LVL: Programmable Logic Controller (PLC) configured for machine control.

[SOURCE:IEC 62061: 2021, 3.2.62]

3.1.40

full variability language

FVL

type of language that provides the capability to implement a wide variety of functions and applications

Note 1 to entry: Typical example of systems using FVL are general-purpose computers.

Note 2 to entry: FVL is normally found in embedded software and is rarely used in application software.

Note 3 to entry: FVL examples include: Ada, C, Pascal, Instruction List, assembler languages, C++, Java, SQL.

[SOURCE:IEC 62061: 2021, 3.2.61]

3.1.41

safety-related application software

SRASW

software specific to the application and generally containing logic sequences, limits and expressions that control the appropriate inputs, outputs, calculations and decisions necessary to meet the safety-related part of a control system (SRP/CS) requirements

3.1.42

safety-related embedded software

SRESW

software that is part of the system supplied by the manufacturer and is not intended for modification by the end-user

Note 1 to entry: Embedded software is also referred to as firmware or system software. See, **full variability language (FVL)** (3.1.40).

[SOURCE:IEC 61511-1:2016, 3.2.76.2]

3.1.43

high demand or continuous mode

mode of operation in which the frequency of demands on a safety-related part of a control system (SRP/CS) to perform its **safety function** (3.1.27) is greater than one per year or the safety function retains the machine in a safe state as part of normal operation

[SOURCE:IEC 61508-4:2010, 3.5.16]

3.1.44

low demand mode

mode of operation in which the frequency of demands on the safety-related part of a control system (SRP/CS) to perform its **safety function** (3.1.27) is not greater than once per year

Note 1 to entry: Low demand mode is not addressed in this document. See Clause 1 for further details.

[SOURCE:IEC 61508-4:2010, 3.5.16, modified - Note 1 to entry has been amended.]

3.1.45

subsystem

entity which results from a first-level decomposition of a safety-related part of a control system (SRP/CS) and whose **dangerous failure** (3.1.12) results in a dangerous failure of a **safety function** (3.1.27)

Note 1 to entry: The subsystem specification includes its role in the safety function and its interface with the other subsystems of the SRP/CS.

Note 2 to entry: One subsystem can be part of one or several SRP/CS, e.g. the same combination of contactors can be used to de-energise a motor in case of detection of a person in a danger zone and also in case of opening a safe guard.

3.1.46

subsystem element

part of a **subsystem** (3.1.45) comprising a single component or any group of components

Note 1 to entry: A subsystem element can comprise hardware or a combination of hardware and software. For the purposes of this document, software-only components are not considered subsystem elements.

Note 2 to entry: For the safety-related values of components or parts of control systems, see Annex O.

3.1.47

channel

element or group of elements that independently implement a **safety function** (3.1.27) or a part of it

Note 1 to entry: Channel can be a functional channel or a testing channel.

[SOURCE:IEC 61508-4:2010, 3.3.6, modified - “or a part of it” has been added to the definition and Note 1 to entry has been added.]

3.1.48

operating mode

mode of operation in a machine (e.g. automatic, manual, maintenance) to select predefined machine functions and safety measures related to those functions

Note 1 to entry: For each specific operating mode, the relevant **safety functions** (3.1.27) and/or risk **reduction measures** (3.1.22) are implemented.

Note 2 to entry: Operating mode is not a machine function itself. The functions (including safety functions) summarized under an operating mode can only be used when that particular operating mode has been activated.

3.1.49

well-tried safety principle

principle that has proved effective in the design or integration of safety-related control systems in the past, to avoid or control critical **faults** (3.1.8) or **failures** (3.1.10) which can influence the performance of a **safety function** (3.1.27)

Note 1 to entry: Newly developed safety principles can only be considered as equivalent to well-tried if they are verified using methods which demonstrate their suitability and reliability for safety-related applications.

Note 2 to entry: Well-tried safety principles are effective not only against random hardware failures, but also against **systematic failures** (3.1.14) which can creep into the product at some point in the course of the product life cycle, e.g. faults arising during product design, integration, modification or deterioration.

Note 3 to entry: ISO 13849-2:2012, Tables A.2, B.2, C.2 and D.2 address well-tried safety principles for different technologies.

3.1.50

well-tried component

component successfully used in safety-related applications

Note 1 to entry: See 6.1.11 for requirements and ISO 13849-2:2012 for a list of recognized well-tried components.

3.1.51

dynamic test

executing either software or operating hardware, or both, in a controlled and systematic way, so as to demonstrate the presence of the required behaviour and the absence of unwanted behaviour

Note 1 to entry: The test fails if **monitoring** (3.1.29) did not detect the change as expected.

Note 2 to entry: The use of test pulses is a common technology of dynamic testing and is widely used to detect short circuits or interruptions in signal paths or malfunctions.

3.1.52

plausibility check

diagnostic measure which is **monitoring** (3.1.29) that the state of an input (output) fits to the state of the system or other inputs (outputs)

3.1.53

verification

confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

Note 1 to entry: The objective evidence needed for a verification can be the result of an inspection or of other forms of determination such as performing alternative calculations or reviewing documents.

Note 2 to entry: The activities carried out for verification are sometimes called a qualification process.

Note 3 to entry: The word "verified" is used to designate the corresponding status.

[SOURCE:ISO 9000:2015, 3.8.12]

3.1.54

validation

confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled

Note 1 to entry: The objective evidence needed for a validation is the result of a test or other form of determination such as performing alternative calculations or reviewing documents.

Note 2 to entry: The word "validated" is used to designate the corresponding status.

Note 3 to entry: The use conditions for validation can be real or simulated.

[SOURCE:IEC 61508-4:2010, 3.8.2]

3.1.55

skilled person

person with relevant training, education, and experience to enable him or her to perceive **risks** (3.1.19) and to avoid **hazards** (3.1.17) associated with the relevant equipment

Note 1 to entry: Several years of practice in the relevant technical field can be taken into consideration in assessment of professional training.

[SOURCE:ISO 14990-1:2016, 3.5.4, modified - “electricity” has been replaced by “the relevant equipment” in the definition and Note 1 to entry has been added.]

3.1.56

black box

device, system or object which can be viewed in terms of its inputs and outputs only

3.1.57

grey box

device, system or object where some of the internal functions are known

Note 1 to entry: The third way for functional testing is “white box”, where all internal functions are known.

3.1.58

average frequency of a dangerous failure per hour

PFH

average frequency of a dangerous failure of a **safety-related part of a control system (SRP/CS)** (3.1.1) to perform the specified safety function over a given period of time

[SOURCE:IEC 61508-4:2010, 3.6.19, modified - “an E/E/PE” has been deleted.]

3.2 Symbols and abbreviated terms

Table 1 - Symbols and abbreviated terms

Symbol or abbreviated term	Description	Subclause or section
a, b, c, d, e	denotation of performance levels	Table K.1
AOPD	active optoelectronic protective device (e.g. light barrier)	Annex H
B, 1, 2, 3, 4	denotation of categories	Table 5
B_{10D}	number of cycles until 10 % of the components fail dangerously (for components with mechanical wear)	Annex C
Cat.	category	3.1.4
CC	current converter	Annex I
CCF	common cause failure	3.1.13
DC	diagnostic coverage	3.1.35
DC_{avg}	average diagnostic coverage	E.2
EMI	electromagnetic interference	F.3.6.1
ETA	event tree analysis	10.3.2
F, F1, F2	frequency and/or exposure times to hazard	A.3.2
FB	function block	Annex J
FVL	full variability language	3.1.40
FMEA	failure modes and effects analysis	6.1.5

Symbol or abbreviated term	Description	Subclause or section
FMECA	failure modes, effects and criticality analysis	10.3.2
FTA	fault tree analysis	10.3.2
$F_D(t)$	cumulated distribution function	C.4.3
HFT	hardware fault tolerance	6.1
I, I1, I2	input device, e.g. sensor	6.1
i, j	index for counting	Annex D
I/O	inputs/outputs	Table E.1
i_m	interconnecting means	Figures 7, 8, 9, 10
K1A, K1B	contactors	Annex I
L, L1, L2	logic	6.1
LVL	limited variability language	3.1.39
λ_D	dangerous failure rate of a component	Annex C
M	motor	Annex I
MTTF	mean time to failure	Annex C
$MTTF_D$	mean time to dangerous failure	3.1.32
MTTR	mean time to restoration	Annex D

Symbol or abbreviated term	Description	Subclause or section
n, N, $\tilde{N}$	number of items	6.2, D.1
N_{low}	number of subsystems with PL_{low} in a combination of subsystems	6.2
n_{op}	mean number of annual operations	Annex C
O, O1, O2, OTE	output device, output of the test equipment, e.g. power control elements	6.1
P, P1, P2	possibility of avoiding or limiting harm	A.3.3
PE system	programmable electronic system	3.1.31, Annex H
PFH	average frequency of a dangerous failure per hour	3.1.58, Table 2, Table K.1
PL	performance level	3.1.5
PLC	programmable logic controller	Annex I
PL_{low}	lowest performance level of a subsystem in a combination of subsystems	6.2
PL_r	required performance level	3.1.6
r_d	demand rate	3.1.38
r_t	test rate	3.1.37
RDF	ratio of dangerous failures	3.1.34
RS	rotation sensor	Annex I
S, S1, S2	severity of injury	A.3.1

Symbol or abbreviated term	Description	Subclause or section
SB	subsystem	Figures 13, H.1, H.2
SOS	safe operating stop	5.2.2.2
SS2	safe stop 2	5.2.2.2
SW1A, SW1B, SW2	position switches	Annex I
SIL	safety integrity level	3.1.7, Clause 6
SLS	safely limited speed	Table 3
SRASW	safety-related application software	3.1.41
SRESW	safety-related embedded software	3.1.42
SRP/CS	safety-related part of a control system	3.1.1
SRS	safety requirements specification	3.1.3
STO	safe torque off	Tables 3 and N.2
TE	test equipment	6.1
T_{M}	mission time	3.1.36
T_{10D}	mean time until 10 % of the components fail dangerously	Annex C

Bibliography

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

[2] ISO 4413:2010, *Hydraulic fluid power - General rules and safety requirements for systems and their components*

[3] ISO 4414:2010, *Pneumatic fluid power - General rules and safety requirements for systems and their components*

[4] ISO 7731:2003, *Ergonomics - Danger signals for public and work areas - Auditory danger signals*

[5] ISO 8573-1, *Compressed air - Part 1: Contaminants and purity classes*

[6] ISO 9000:2015, *Quality management systems - Fundamentals and vocabulary*

[7] ISO 9001:2015, *Quality management systems - Requirements*

[8] ISO 9241-210, *Ergonomics of human-system interaction - Part 210: Human-centred design for interactive systems*

[9] ISO 10218-1:2011, *Robots and robotic devices - Safety requirements for industrial robots - Part 1: Robots*

[10] ISO 10218-2, *Robots and robotic devices - Safety requirements for industrial robots - Part 2: Robot systems and integration*

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

[12] ISO 11428:1996, *Ergonomics - Visual danger signals - General requirements, design and testing*

[13] ISO 11429:1996, *Ergonomics - System of auditory and visual danger and information signals*

[14] ISO 13850:2015, *Safety of machinery - Emergency stop function - Principles for design*

[15] ISO 13851, *Safety of machinery - Two-hand control devices - Principles for design and selection*

[16] ISO 13856-1, *Safety of machinery - Pressure-sensitive protective devices - Part 1: General principles for design and testing of pressure-sensitive mats and pressure-sensitive floors*

[17] ISO 13856-2, *Safety of machinery - Pressure-sensitive protective devices - Part 2: General principles for design and testing of pressure-sensitive edges and pressure-sensitive bars*

[18] ISO 14118:2017, *Safety of machinery - Prevention of unexpected start-up*

[19] ISO 14119:2013, *Safety of machinery - Interlocking devices associated with guards - Principles for design and selection*

[20] ISO/TR 14121-2, *Safety of machinery - Risk assessment - Part 2: Practical guidance and examples of methods*

[21] ISO/TS 15066:2016, *Robots and robotic devices - Collaborative robots*

[22] ISO 16090-1, *Machine tools safety - Machining centres, Milling machines, Transfer machines - Part 1: Safety requirements*

[23] ISO 19973 (all parts), *Pneumatic fluid power - Assessment of component reliability by testing*

[24] ISO/TR 22100-2:2013, *Safety of machinery - Relationship with ISO 12100 - Part 2: How ISO 12100 relates to ISO 13849-1*

[25] ISO/TR 22100-3, *Safety of machinery - Relationship with ISO 12100 - Part 3: Implementation of ergonomic principles in safety standards*

[26] ISO/TR 22100-4, *Safety of machinery - Relationship with ISO 12100 - Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects*

[27] ISO 23125, *Machine tools - Safety - Turning machines*

[28] ISO/IEC/IEEE 26512, *Systems and software engineering - Requirements for acquirers and suppliers of information for users*

[29] EN 614-1, *Safety of machinery - Ergonomic design principles - Part 1: Terminology and general principles*

[30] EN 1005-3, *Safety of machinery - Human physical performance - Part 3: Recommended force limits for machinery operation*

[31] EN 50178, *Electronic equipment for use in power installations*

[32] IEC 60204-1:2016+AMD1:2021, *Safety of machinery - Electrical equipment of machines - Part 1: General requirements*

[33] IEC 60447, *Basic and safety principles for man-machine interface (MMI) - Actuating principles*

[34] IEC 60050-192:2015, *International electrotechnical vocabulary - Part 192: Dependability*

[35] IEC 60529, *Degrees of protection provided by enclosures (IP code)*

[36] IEC 60812, *Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)*

[37] IEC 60947 (all parts), *Low-voltage switchgear and controlgear*

[38] IEC 60950-1, *Information technology equipment - Safety - Part 1: General requirements*

[39] IEC 61000-1-2, *Electromagnetic compatibility (EMC) - Part 1-2: General - Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena*

[40] IEC 61000-6-2, *Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity for industrial environments*

[41] IEC 61000-6-7:2014, *Electromagnetic compatibility (EMC) - Part 6-7: Generic standards - Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial locations*

[42] IEC 61025, *Fault tree analysis (FTA)*

[43] IEC 61078, *Reliability block diagrams*

[44] IEC 61300 (all parts), *Fibre optic interconnecting devices and passive components - Basic test and measurement procedures*

[45] IEC 61310 (all parts), *Safety of machinery - Indication, marking and actuation*

[46] IEC 61131-3:2013, *Programmable controllers - Part 3: Programming languages*

[47] IEC 61310-1:2007, *Safety of machinery - Indication, marking and actuation - Part 1: Requirements for visual, acoustic and tactile signals*

[48] IEC 61326-3-1, *Electrical equipment for measurement, control and laboratory use - EMC requirements - Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) - General industrial applications*

[49] IEC 61496-1:2020, *Safety of machinery - Electro-sensitive protective equipment - Part 1: General requirements and tests*

[50] IEC 61496-2, *Safety of machinery - Electro-sensitive protective equipment - Part 2: Particular requirements for equipment using active opto-electronic protective devices*

[51] IEC 61496-3, *Safety of machinery - Electro-sensitive protective equipment - Part 3: Particular requirements for active opto-electronic protective devices responsive to diffuse reflection (AOPDDR)*

[52] IEC 61506, *Industrial-process measurement and control - Documentation of software for process control systems and facilities*

[53] IEC 61508-1, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements*

[54] IEC 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

[55] IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations*

[56] IEC 61508-5, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 5: Examples of methods for the determination of safety integrity levels*

[57] IEC 61508-6:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

[58] IEC 61508-7:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures*

[59] IEC 61511-1:2016, *Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and application programming requirements*

[60] IEC 61558-2-16, *Safety of transformers, reactors, power supply units and combinations thereof - Part 2-16: Particular requirements and tests for switch mode power supply units and transformers for switch mode power supply units for general applications*

[61] IEC 61709,[2] *Electric components - Reliability - Reference conditions for failure rates and stress models for conversion*

[62] IEC 61784 (all parts), *Industrial communication networks - Profiles*

[63] IEC 61800-3, *Adjustable speed electrical power drive systems - Part 3: EMC requirements and specific test methods*

[64] IEC 61800-5-2:2016, *Adjustable speed electrical power drive systems - Part 5-2: Safety requirements - Functional*

[65] IEC 61810-2-1, *Electromechanical elementary relays - Part 2-1: Reliability - Procedure for the verification of* B_{10} *values*

[66] IEC 61810-3, *Electromechanical elementary relays - Part 3: Relays with forcibly guided (mechanically linked) contacts*

[67] IEC 62021 (all parts), *Insulating liquids - Determination of acidity*

[68] IEC 62024 (all parts), *High frequency inductive components - Electrical characteristics and measuring methods*

[69] IEC 62368-1, *Audio/video, information and communication technology equipment - Part 1: Safety requirements*

[70] IEC 62502, *Analysis techniques for dependability - Event tree analysis (ETA)*

[71] IEC/TR 63074, *Safety of machinery - Security aspects related to functional safety of safety-related control systems*

[72] EN 50495:2010, *Safety devices required for the safe functioning of equipment with respect to explosion risks*

[73] ANSI B11.26:2018 *Functional Safety for Equipment: General Principles for the Design of Safety Control Systems Using ISO 13849-1*

[74] SN 29500 (all parts), *Failure rates of components, Edition 1999-11, Siemens AG 1999s*

[75] VDMA 66413, *Functional Safety - Universal data format for safety-related values of components or parts of control system*

[76] VDMA 24584:2020, *Safety functions of regulated and unregulated (fluid) mechanical systems*

[77] Goble W.M., Control systems Safety Evaluation and Reliability. 3rd Edition:2010 (ISBN-101934394807)

[78] IFA-Report 2/2017e, *Functional safety of machine controls – Application of ISO 13849*, German Social Accident Insurance (DGUV), June 2009, ISBN 978-3-88383-793-2, free download in the Internet: www.dguv.de/ifa/13849e

[79] Chinniah Yuvin, 2015) Analysis and prevention of serious and fatal accidents related to moving parts of machinery, Safety Science 75 (2015) 163–173

[80] Haghighi A., Jocelyn S., Chinniah Y., "Testing and Improving an ISO 14119-Inspired Tool to Prevent Bypassing Safeguards on Industrial Machines"; Safety, volume 6, issue 3, 2020 https://www.mdpi.com/2313-576X/6/3/42

[81] IFA. "*SISTEMA Cookbook 6: Definition of safety functions: what is important?*" (https://www.dguv.de/webcode.jsp?query=e109249)

[82] *Reliability Prediction of Electronic Equipment, MIL-HDBK-217E*, Notice-2, Department of Defense, Washington, DC, 1995

[83] *British Handbook for Reliability Data for Components used in Telecommunication Systems*, British Telecom (HRD5, last issue)

[84] Chinese Military Standard, GJB/Z 299C-2006 *Reliability prediction handbook for electronic equipment (English Version*)

[85] *EMC The easy way*, Pocket guide, published by Division of Switching Devices, Switchboards and Industrial Controls of the ZVEI (German Electrical and Electronic Manufacturer's Association), Frankfurt/Main, Germany (https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2008/Januar/EMC-Pocket-Guide-ZVEI-english.pdf)

[2] Identical to RDF 2000/*Reliability Data Handbook*, UTE C 80-810, Union Technique de l'Electricité et de la Communication.

…

Fonte: ISO