Deleted:

ISO/FDIS 13849-1:2022(E)

2022-08

Deleted: 07-19

ISO TC 199/WG 8

Secretariat: DIN

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

Sécurité des machines — Parties des systèmes de commande relatives à la sécurité — Partie 1: Principes généraux de conception

ISO copyright office

CP 401 • Ch. de Blandonnet 8

CH-1214 Vernier, Geneva

Phone: +41 22 749 01 11

Fax: +41 22 749 09 47

Email: copyright@iso.org

Website: www.iso.org

Published in Switzerland

Deleted:

Contents

Deleted:

Deleted:

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 144, *Safety of machinery*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

Deleted: .

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);

Deleted:

— 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.

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.

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.

Deleted: hands

Deleted: .

Deleted: in case of

Deleted: it is the intent that

Deleted: being

Deleted: <object>

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.

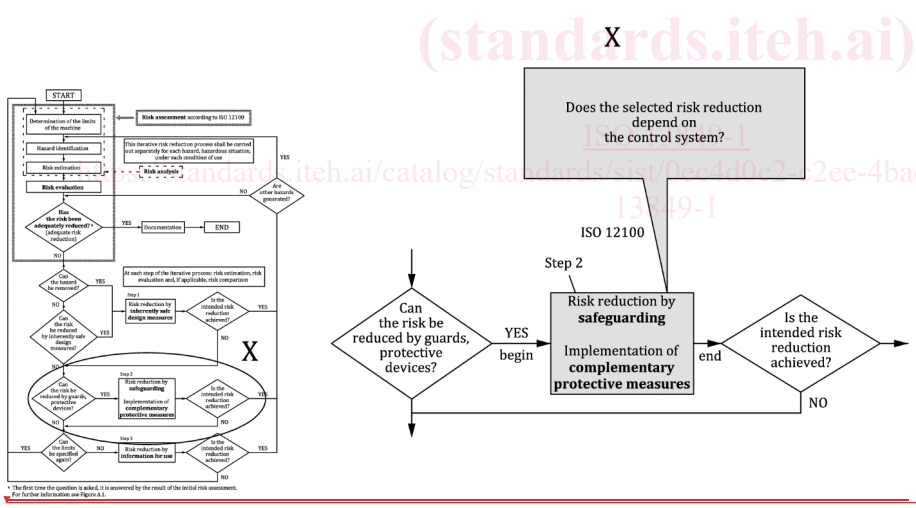
Risk reduction according to ISO 12100:2010, Clause 6, is accomplished by applying, in the following sequence, inherently safe design measures, safeguarding and/or complementary risk reduction measures and information for use. A designer can reduce risks by risk reduction measures that can have safety 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 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 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 and this document. For a detailed overview see Figure 2.

Deleted: , taken from ISO 22100-2:2013,

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



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

Deleted:

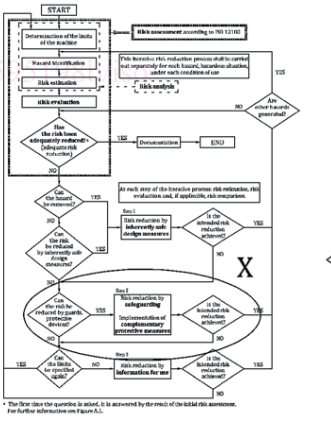


Figure 1 — Integration of this document (ISO 13849-1) within the risk reduction process of ISO 12100

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.

Deleted: faults

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).

Deleted: DIS

Deleted: .2:2021

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

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.

Deleted: , requirements

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.

Deleted: -

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*

Deleted: 2021

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:

Deleted: terminological

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

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

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 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.]

Deleted: NOTES deleted and

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).