INTERNATIONAL STANDARD

ISO 13849-1

Redline version
compares Fourth edition to
Third edition

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

Reference number
ISO13849-1:redline:2023(E)

IMPORTANT — PLEASE NOTE

This is a provisional mark-up copy and uses the following colour coding:

Text example 1	— indicates added text (in green)
~~Text example 2~~	— indicates removed text (in red)
□	— indicates added graphic figure
☒	— indicates removed graphic figure
1.x ...	— Heading numbers containg modifications are highlighted in yellow in the Table of Contents

All changes in this document have yet to reach concensus by vote and as such should only be used internally for review purposes.

DISCLAIMER

This Redline version is not an official IEC Standard and is intended only to provide the user with an indication of what changes have been made to the previous version. Only the current version of the standard is to be considered the official document.

This Redline version provides you with a quick and easy way to compare all the changes between this standard and its previous edition. A vertical bar appears in the margin wherever a change has been made. Additions and deletions are displayed in red, with deletions being struck through.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword vii
Introduction ix
1 Scope 1
2 Normative references 2
3 Terms, definitions, symbols and abbreviated terms 2
3.1 Terms and definitions 2
3.2 Symbols and abbreviated terms 14
~~4 Design considerations~~ 16
4 Overview 16
~~4.1 Safety objectives in design~~ 16
4.1 Risk assessment and risk reduction process at the machine 16
4.2 ~~Strategy for~~ Contribution to the risk reduction 19
~~4.2.1 General~~ 19
~~4.2.2 Contribution to the risk reduction by the control system~~ 19
~~4.3 Determination of required performance level (PL_r)~~ 23
4.3 Design process of an SRP/CS 23
~~4.4 Design of SRP/CS~~ 24
~~4.5 Evaluation of the achieved performance level PL and relationship with SIL~~ 25
~~4.5.1 Performance level PL~~ 25
~~4.5.2 Mean time to dangerous failure of each channel ($MTTF_D$)~~ 27
~~4.5.3 Diagnostic coverage (DC)~~ 28
~~4.5.4 Simplified procedure for estimating the quantifiable aspects of PL~~ 28
~~4.5.5 Description of the output part of the SRP/CS by category~~ 31
4.4 Methodology 31
~~4.6 Software safety requirements~~ 32
~~4.6.1 General~~ 32
~~4.6.2 Safety-related embedded software (SRESW)~~ 33
~~4.6.3 Safety-related application software (SRASW)~~ 34
~~4.6.4 Software-based parameterization~~ 36
~~4.7 Verification that achieved PL meets PL_r~~ 37
4.5 Required information 38
~~4.8 Ergonomic aspects of design~~ 38
4.6 Safety function realization by using subsystems 38
5 ~~Safety~~ Specification of safety functions 39
~~5.1 Specification of safety functions~~ 39
5.1 Identification and general description of the safety function 40
~~5.2 Details of safety functions~~ 43
5.2 Safety requirements specification 43
~~5.2.1 Safety-related stop function~~ 43
5.2.1 General requirements 43
~~5.2.2 Manual reset function~~ 46
5.2.2 Requirements for specific safety functions 46
~~5.2.3 Start/restart function~~ 50
5.2.3 Minimizing motivation to defeat safety functions 50
~~5.2.4 Local control function~~ 51
5.2.4 Remote access 51
~~5.2.5 Muting function~~ 51
~~5.2.6 Response time~~ 52
~~5.2.7 Safety-related parameters~~ 52
~~5.2.8 Fluctuations, loss and restoration of power sources~~ 52
5.3 Determination of required performance level (PL_r) for each safety function 52
5.4 Review of the safety requirements specification (SRS) 52

5.5 Decomposition of SRP/CS into subsystems 53

~~6 Categories and their relation to MTTF$_D$ of each channel, DC$_{avg}$ and CCF~~ 54
~~6.1 General~~ 54

6 Design considerations **55**
~~6.2 Specifications of categories~~ 55
6.1 Evaluation of the achieved performance level 55
~~6.2.1~~ 6.1.1 General overview of performance level 55
~~6.2.2 Designated architectures~~ 57
6.1.2 Correlation between performance level (PL) and safety integrity level (SIL) 57
~~6.2.3 Category B~~ 57
~~6.2.4 Category 1~~ 58
~~6.2.5 Category 2~~ 59
6.1.3 Architecture — Categories and their relation to MTTF$_D$ of each channel, average diagnostic coverage and common cause failure (CCF) 60
~~6.2.6 Category 3~~ 68
6.1.4 Mean time to dangerous failure (MTTF$_D$) 68
6.1.5 Diagnostic coverage (DC) 70
6.1.6 Common cause failures (CCFs) 71
6.1.7 Systematic failures 71
6.1.8 Simplified procedure for estimating the performance level for subsystems 71
6.1.9 Alternative procedure to determine the performance level and PFH without MTTF$_D$ 73
~~6.2.7 Category 4~~ 74
6.1.10 Fault consideration and fault exclusion 77
6.1.11 Well-tried component 78
~~6.3~~ 6.2 Combination of ~~SRP/CS~~ subsystems to achieve ~~overall PL~~ an overall performance level of the safety function 79
6.2.1 General 80
6.2.2 Known PFH values 80
6.2.3 Unknown PFH values 81
6.3 Software based manual parameterization 81
6.3.1 General 81
6.3.2 Influences on safety-related parameters 82
6.3.3 Requirements for software based manual parameterization 82
6.3.4 Verification of the parameterization tool 83
6.3.5 Documentation of software based manual parameterization 84

~~7 Fault consideration, fault exclusion~~ **84**

7 Software safety requirements **84**
7.1 General 84
~~7.2 Fault consideration~~ 86
7.2 Limited variability language (LVL) and full variability language (FVL) 86
7.2.1 Limited variability language (LVL) 86
7.2.2 Full variability language (FVL) 86
7.2.3 Decision for limited variability language (LVL) or full variability language (FVL) 87
7.3 Safety-related embedded software (SRESW) 88
7.3.1 Design of safety-related embedded software (SRESW) 88
7.3.2 Alternative procedures for non-accessible embedded software 89
~~7.3 Fault exclusion~~ 89
7.4 Safety-related application software (SRASW) 89

8 Verification of the achieved performance level **92**

9 Ergonomic aspects of design **92**

~~8~~ 10 Validation 93
10.1 Validation principles 93
10.1.1 General 93
10.1.2 Validation plan 95
10.1.3 Generic fault lists 96
10.1.4 Specific fault lists 96
10.1.5 Information for validation 96
10.2 Validation of the safety requirements specification (SRS) 97
10.3 Validation by analysis 98
10.3.1 General 98
10.3.2 Analysis techniques 98
10.4 Validation by testing 98
10.4.1 General 98
10.4.2 Measurement accuracy 99
10.4.3 Additional requirements for testing 100
10.4.4 Number of test samples 100
10.4.5 Testing methods 100
10.5 Validation of the safety functions 101
10.6 Validation of the safety integrity of the SRP/CS 101
10.6.1 Validation of subsystem(s) 101
10.6.2 Validation of measures against systematic failures 102
10.6.3 Validation of safety-related software 103
10.6.4 Validation of combination of subsystems 104
10.6.5 Overall validation of safety integrity 104
10.7 Validation of environmental requirements 104
10.8 Validation record 105
10.9 Validation maintenance requirements 105

~~9 Maintenance~~ 105

11 Maintainability of SRP/CS 105

~~10~~ 12 Technical documentation 106

~~11~~ 13 Information for use 107
13.1 General 108
13.2 Information for SRP/CS integration 108
13.3 Information for user 108

Annex A (informative) ~~Determination~~ Guidance for the determination of required performance level (PL_r) 110

Annex B (informative) Block method and safety-related block diagram 117

Annex C (informative) Calculating or evaluating $MTTF_D$ values for single components 119

Annex D (informative) Simplified method for estimating $MTTF_D$ for each channel 131

Annex E (informative) Estimates for diagnostic coverage (DC) for functions and ~~modules~~ subsystems 134

Annex F (informative) ~~Estimates for common cause failure (CCF)~~ Method for quantification of measures against common cause failures (CCF) 138

Annex G (informative) Systematic failure 143

Annex H (informative) Example of a combination of several ~~safety-related partsof the control system~~ subsystems 147

Annex I (informative) Examples for the simplified procedure to estimate the PL of subsystems 151

Annex J (informative) ~~Software~~ Example of SRESW realisation 163

Annex K (informative) Numerical representation of Figure ~~5~~ 12 169

Annex L (informative) **Electromagnetic interference (EMI) immunity** 173
Annex M (informative) **Additional information for safety requirements specification (SRS)** 177
Annex N (informative) **Avoiding systematic failure in software design** 179
Annex O (informative) **Safety-related values of components or parts of control systems** 199
Bibliography 202

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~~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~~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 ~~on the~~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~~ISO’s adherence to the ~~WTO~~World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) ~~see the following URL.~~, see ~~Foreword - Supplementary information~~www.iso.org/iso/foreword.html.

~~The committee responsible for this document is ISO/TC 199, *Safety of machinery*~~.

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 ~~third~~fourth edition cancels and replaces the ~~second~~third edition (ISO 13849-1:~~2006~~2015), which has been technically revised. ~~It also incorporates Technical Corrigendum ISO 13849-1:2006/Cor 1:2009. Changes from the previous edition include~~

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;

~~— deletion of the former Table 1 from the Introduction;~~

— specification of the safety functions (updated Clause 5);

~~— updating and addition of normative references;~~

— combination of several subsystems (updated in Clause 6);

~~— modification of the definitions of terms *hazardous situation* and *high demand or continuous mode*;~~

— new Clause 7 on software safety requirements;

— new Clause 9 on ergonomic aspects of design;

— validation (updated Clause 8 and moved to Clause 10);

- ~~addition of a new term and definition, *proven in use*,~~
- new G.5 on management of the functional safety;
- new Annex L on electromagnetic interference (EMI) immunity;
- ~~editorial, but not technical, modification of Figure 1,~~
- new Annex M with additional information for safety requirements specification;
- ~~a new subclause, 4.5.5, as well as modifications to existing sections including the annexes, substantial modification of Annex G and an entirely new Annex I.~~
- 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.

~~ISO 13849 consists of the following parts, under the general title *Safety of machinery — Safety-related parts of control systems*:~~

- ~~*Part 1: General principles for design*~~
- ~~*Part 2: Validation*~~

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-~~hands~~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.

~~c) Type-C standards (machinery safety standards) deal with detailed safety requirements for a particular machine or group of machines.~~

This ~~part of~~document ~~ISO 13849~~is a type-~~B-1~~B1 standard as ~~stated~~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 ~~representing the market players~~ with regard to machinery safety:

— machine manufacturers (small, medium and large enterprises);

— health and safety bodies (regulators, accident prevention organisations, market surveillance~~ etc.~~).

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

— machine users/employers (small, medium and large enterprises);

— machine users/employees (e.g. trade unions~~, organizations for people with special needs~~);

— service providers, ~~e. g.~~e.g. for maintenance (small, medium and large enterprises);

— consumers (i.e. machinery intended for use by consumers).

~~— consumers (in case of machinery intended for use by consumers).~~

The above-mentioned stakeholder groups have been given the possibility to participate ~~at~~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.

~~When provisions of a type-C standard are different from those which are stated in type-A or type-B standards, the provisions of the type-C standard take precedence over the provisions of the other~~

~~standards for machines that have been designed and built according to the provisions of the type-C standard.~~

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 ~~part of~~document ~~ISO 13849~~is intended to give guidance to those involved in the design and assessment of control systems, and ~~to Technical Committees~~those preparing type-B2 or type-C standards~~ which are presumed to comply with the Essential Safety Requirements of Annex I of the Directive 2006/42/EC on machinery. It does not give specific guidance for compliance with other EC directives.~~.

~~As part of the overall risk reduction strategy at a machine, a designer will often choose to achieve some measure of risk reduction through the application of safeguards employing one or more safety functions.~~

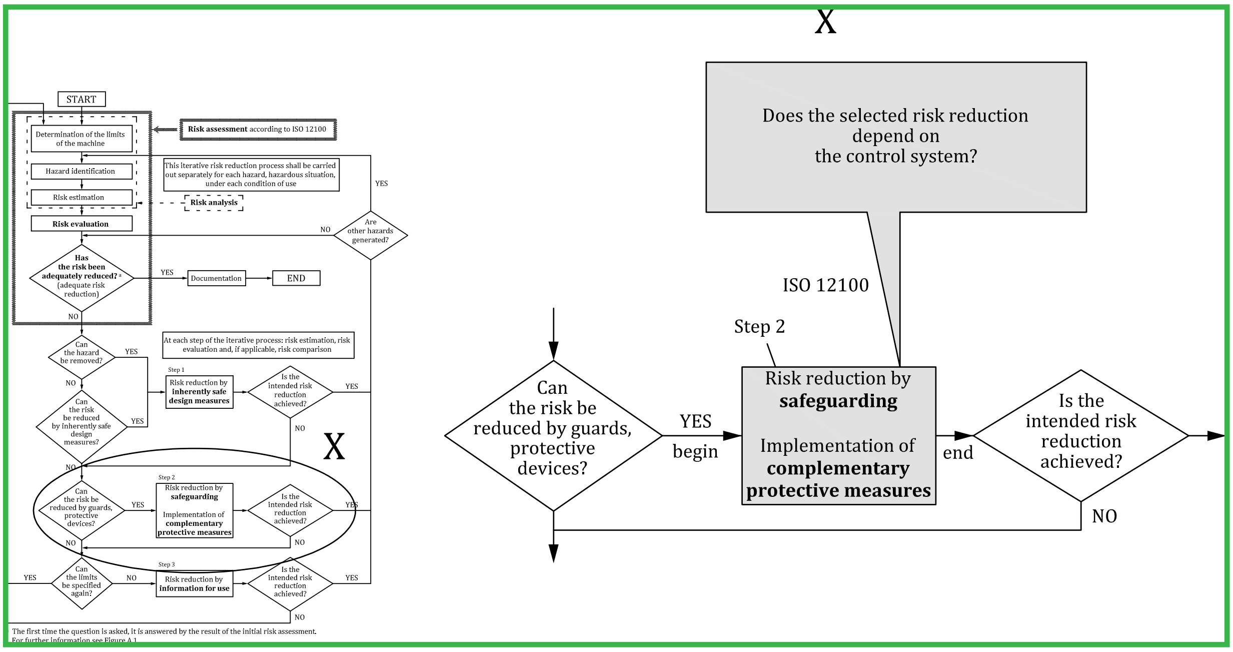
Risk reduction according to ISO 12100:2010, Clause 6, is accomplished by applying, in the following sequence, inherently safe design measures, safeguarding and/or complementary risk reduction measures and information for use. A designer can reduce risks by risk reduction measures that can have safety functions. Parts of machinery control systems that are assigned to provide safety functions are called safety-related parts of control systems (SRP/CS)~~ and these~~. 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 ~~providing~~implementing safety functions, SRP/CS can also ~~provide~~implement operational functions~~ (e.g. two-handed controls as a means of process initiation)~~.

~~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). These performance levels are defined in terms of probability of dangerous failure per hour (see Table 2)~~.

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$_{\text{r}}$) of a safety function performed by the SRP/CS, where its PL$_{\text{r}}$ 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.


START
Risk assessment according to ISO 12100
Determination of the limits of the machine
Hazard identification
Risk estimation
Risk analysis
Risk evaluation
This iterative risk reduction process shall be carried out separately for each hazard, hazardous situation, under each condition of use
Are other hazards generated?
YES
NO
Has the risk been adequately reduced? a (adequate risk reduction)
YES
Documentation
END
NO
At each step of the iterative process: risk estimation, risk evaluation and, if applicable, risk comparison
Can the hazard be removed?
YES
NO
Step 1
Risk reduction by inherently safe design measures
Is the intended risk reduction achieved?
YES
NO
Can the risk be reduced by inherently safe design measures?
YES
NO
X
Step 2
Can the risk be reduced by guards, protective devices?
YES
Risk reduction by safeguarding
Implementation of complementary protective measures
Is the intended risk reduction achieved?
YES
NO
NO
Step 3
YES
Can the limits be specified again?
NO
Risk reduction by information for use
Is the intended risk reduction achieved?
YES
NO
X
Does the selected risk reduction depend on the control system?
ISO 12100
Step 2
Can the risk be reduced by guards, protective devices?
YES
begin
Risk reduction by safeguarding
Implementation of complementary protective measures
end
Is the intended risk reduction achieved?
NO

a The first time the question is asked, it is answered by the result of the initial risk assessment.
For further information see Figure A.1

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

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

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 ~~probability~~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 ~~assist the designer and facilitate~~facilitate the design of SRP/CS and the assessment of achieved PL, this document employs a methodology based on the categorization of ~~structures according to~~architectures with specific design criteria (e.g. MTTF$_D$, DC$_{avg}$) and specified ~~behaviours~~behaviour under fault conditions. These ~~categories~~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 ~~safety-related parts of control systems, such as~~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)~~, electro-sensitive protective devices (e.g. photoelectric barriers), pressure sensitive devices,~~;

— power control ~~units~~elements (e.g. ~~a logic unit for control functions, data processing, monitoring, etc.), and~~relays, valves);

— ~~power control~~sensors and HMI elements (e.g. ~~relays, valves, etc.),~~position sensors, enable switches).

~~as well as to control systems carrying out safety functions at all kinds of machinery —~~Machinery covered by this document can range from simple (e.g. small kitchen machines, or automatic doors and gates) to ~~manufacturing installations~~complex (e.g. packaging machines, printing machines, presses and integrated machinery into a system).

~~This part of ISO 13849 is intended to provide a clear basis upon which the design and performance of any application of the SRP/CS (and the machine) can be assessed, for example, by a third party, in-house or by an independent test house.~~

~~Information on the recommended application of IEC 62061 and this part of ISO 13849~~

This document and IEC 62061 ~~and this part of~~both specify a methodology and provide related guidance ~~ISO 13849 specify requirements~~ for the design and implementation of safety-related control systems of machinery. ~~The use of either of these International Standards, in accordance with their scopes, can be presumed to fulfil the relevant essential safety requirements. ISO/TR 23849 gives guidance on the application of this part of ISO 13849 and IEC 62061 in the design of safety-related control systems for machinery.~~

~~As with ISO/TR 23849, ISO/TR 22100-2 has been added to the list of normative references given in Clause 2 — the latter owing to its importance for an understanding of the relationship between this part of ISO 13849 and ISO 12100.~~

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

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.

This ~~part of~~document ~~ISO 13849 provides safety requirements and guidance on the principles for the design and integration of safety-related parts of control systems (SRP/CS), including the design of software. For these parts of SRP/CS, it specifies characteristics that include the performance level required for carrying out safety functions. It~~ applies to SRP/CS for high demand and continuous ~~mode~~modes of operation including their subsystems, regardless of the type of technology and energy ~~used~~ (e.g. electrical, hydraulic, pneumatic, ~~mechanical, etc.), for all kinds of machinery~~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.

~~It~~This document does not specify the safety functions or required performance levels (PL$_r$) that are to be used in ~~a~~ particular ~~case~~applications.

~~This part of ISO 13849 provides specific requirements for SRP/CS using programmable electronic system(s).~~

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.

~~It~~This document does not give specific requirements for the design of products~~ which~~/components that are parts of SRP/CS. ~~Nevertheless, the principles given, such as categories or performance levels, can be used~~Specific requirements for the design of some components of SRP/CS are covered by applicable ISO and IEC standards.

~~NOTE 1 Examples of products which are parts of SRP/CS: relays, solenoid valves, position switches, PLCs, motor control units, two-hand control devices, pressure sensitive equipment. For the design of such products, it is important to refer to the specifically applicable International Standards, e.g. ISO 13851, ISO 13856-1 and ISO 13856-2.~~

~~NOTE 2 For the definition of *required performance level*, see 3.1.24.~~

~~NOTE 3 The requirements provided in this part of ISO 13849 for programmable electronic systems are compatible with the methodology for the design and development of safety-related electrical, electronic and programmable electronic control systems for machinery given in IEC 62061.~~

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

NOTE ~~4~~ 3 ~~For safety-related embedded software for components with PL$_r$ = e, see IEC 61508-3:1998, Clause 7.~~ 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~~, in whole or in part, are normatively referenced in this document and are indispensable for its application~~ 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*

~~IEC 60050-191:1990, , *International electrotechnical vocabulary — Chapter 191: Dependability and quality of service*. Amended by IEC 60050-191-am1:1999 and IEC 60050-191-am2:2002:1999~~

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*. ~~Corrected by IEC 61508-3/Cor.1:1999~~

~~IEC 61508-4:2010, , *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations*. Corrected by IEC 61508-4/Cor.1:1999~~

IEC 62046:2018, , *Safety of machinery — Application of protective equipment to detect the presence of persons*

IEC 62061:~~2012~~ 2021, *Safety of machinery — Functional safety of safety~~-related electrical, electronic and programmable electronic~~ -related control systems*

~~ISO/TR 22100-2:2013~~IEC/IEEE 82079-1:2019, ~~*Safety of machinery — Relationship with ISO 12100 — Part 2: How ISO 12100 relates to ISO 13849-1*~~, *Preparation of information for use (instructions for use) of products — Part 1: Principles and general requirements*

~~ISO/TR 23849, , *Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery*~~

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 ~~IEC 60050-191 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 ~~responds to~~ performs a *safety function* (3.1.27), starting from a safety-related input ~~signals and generates~~ (s) to generating a safety-related output ~~signals~~ (s)

Note 1 to entry: The ~~combined~~ safety-related parts of a control system start at the point where the safety-related ~~input signals~~ 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).

~~Note 2 to entry: If monitoring systems are used for diagnostics, they are also considered as SRP/CS.~~

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.]

~~**3.1.2**~~
3.1.4
category
classification of the ~~safety-related~~ *subsystem* (3.1.45) ~~parts of a control system in respect of their resistance to faults~~ in respect to its resistance to *faults* (3.1.8) and ~~their~~ the subsequent behaviour in the fault condition, ~~and~~ 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.]