



BSI Standards Publication

Safety of machinery — Safety-related parts of control systems

Part 1: General principles for design

National foreword

This British Standard is the UK implementation of EN ISO 13849-1:2023. It is identical to ISO 13849-1:2023. It supersedes BS EN ISO 13849-1:2015, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee MCE/3, Safeguarding of machinery.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication has been prepared under a mandate given to the European Standards Organizations by the European Commission and the European Free Trade Association. It is intended to support requirements of the EU legislation detailed in the European Foreword. A European Annex, usually Annex ZA or ZZ, describes how this publication relates to that EU legislation.

For the Great Britain market (England, Scotland and Wales), if UK Government has designated this publication for conformity with UKCA marking (or similar) legislation, it may contain an additional National Annex. Where such a National Annex exists, it shows the correlation between this publication and the relevant UK legislation. If there is no National Annex of this kind, the relevant Annex ZA or ZZ in the body of the European text will indicate the relationship to UK regulation applicable in Great Britain. References to EU legislation may need to be read in accordance with the UK designation and the applicable UK law. Further information on designated standards can be found at www.bsigroup.com/standardsandregulation.

For the Northern Ireland market, UK law will continue to implement relevant EU law subject to periodic confirmation. Therefore Annex ZA/ZZ in the European text, and references to EU legislation, are still valid for this market.

UK Government is responsible for legislation. For information on legislation and policies relating to that legislation, consult the relevant pages of www.gov.uk.

© The British Standards Institution 2023
Published by BSI Standards Limited 2023

ISBN 978 0 580 98533 1

ICS 13.110; 29.020

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 May 2023.

Amendments/corrigenda issued since publication

Date

Text affected

English Version

Safety of machinery - Safety-related parts of control
systems - Part 1: General principles for design (ISO 13849-
1:2023)

Sécurité des machines - Parties des systèmes de
commande relatives à la sécurité - Partie 1: Principes
généraux de conception (ISO 13849-1:2023)

Sicherheit von Maschinen - Sicherheitsbezogene Teile
von Steuerungen - Teil 1: Allgemeine
Gestaltungsleitsätze (ISO 13849-1:2023)

This European Standard was approved by CEN on 3 March 2023.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

European foreword

This document (EN ISO 13849-1:2023) has been prepared by Technical Committee ISO/TC 199 "Safety of machinery" in collaboration with Technical Committee CEN/TC 114 "Safety of machinery" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by November 2023, and conflicting national standards shall be withdrawn at the latest by May 2026.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

This document supersedes EN ISO 13849-1:2015.

This document has been prepared under a Standardization Request given to CEN by the European Commission and the European Free Trade Association, and supports essential requirements of EU Directive(s) / Regulation(s).

For the relationship with EU Directive(s) / Regulation(s), see informative Annex ZA, which is an integral part of this document.

Any feedback and questions on this document should be directed to the users' national standards body/national committee. A complete listing of these bodies can be found on the CEN website.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Endorsement notice

The text of ISO 13849-1:2023 has been approved by CEN as EN ISO 13849-1:2023 without any modification.

Annex ZA (informative)

Relationship between this European Standard and the essential requirements of EU Directive 2006/42/EC aimed to be covered

This European Standard has been prepared under a Commission's standardization request M/396 Mandate to CEN and CENELEC for Standardisation in the field of machinery" to provide one voluntary means of conforming to essential requirements of Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast).

Once this standard is cited in the Official Journal of the European Union under that Directive, compliance with the normative clauses of this standard given in Table ZA.1 confers, within the limits of the scope of this standard, a presumption of conformity with the corresponding essential requirements of that Directive, and associated EFTA regulations.

Table ZA.1 — Correspondence between this European Standard and Directive 2006/42/EC

The relevant essential Requirements of Directive 2006/42/EC	Clause(s)/subclause(s) of this EN	Remarks/Notes
1.1.6	9	
1.2.1	6, 7, 10	
1.2.3	5.2.2.4	This subclause only deals with the restart function
1.2.4.1	5.2.2.2	This subclause only deals with those safety-related stop function achieving stop category 0 or 1.
1.2.4.2	5.2.2.2	This subclause only deals with those safety-related stop function achieving stop category 2.
1.2.4.3	5.2.1	This subclause only deals with the safety requirements specification (SRS) of an emergency stop function
1.2.5	5.2.2.9	
1.2.6	5.2.1.3 item i), 5.2.2.8	
1.6.1	11	
1.6.2	11	
1.6.4	11	
1.7.4.2 (e, g, i, r, s)	13	This subclause only deals with the instruction for safety functions.

Table ZA.2 — Applicable Standards to confer presumption of conformity as described in this Annex ZA

Reference in Clause 2	International Standard Edition	Title	Corresponding European Standard Edition
ISO 12100:2010	ISO 12100:2010	<i>Safety of machinery — General principles for design — Risk assessment and risk reduction</i>	EN ISO 12100:2010
ISO 13849-2:2012	ISO 13849-2:2012	<i>Safety of machinery — Safety-related parts of control systems — Part 2: Validation</i>	EN ISO 13849-2:2012
ISO 13855:2010	ISO 13855:2010	<i>Safety of machinery — Positioning of safeguards with respect to the approach of the human body</i>	EN ISO 13855:2010
ISO 20607:2019	ISO 20607:2019	<i>Safety of machinery — Instruction handbook — General drafting principles</i>	EN ISO 20607:2019
IEC 61508-3:2010	IEC 61508-3:2010	<i>Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements</i>	IEC 61508-3:2010
IEC 62046:2018	IEC 62046:2018	<i>Safety of machinery — Application of protective equipment to detect the presence of persons</i>	EN IEC 62046:2018
IEC 62061:2021	IEC 62061:2021	<i>Safety of machinery — Functional safety of safety-related control systems</i>	EN IEC 62061:2021
IEC/IEEE 82079-1:2019	IEC/IEEE 82079-1:2019	<i>Preparation of information for use (instructions for use) of products — Part 1: Principles and general requirements</i>	EN IEC/IEEE 82079-1:2019

The documents listed in the Column 1 of Table ZA.2, in whole or in part, are normatively referenced in this document, i.e. are indispensable for its application. The achievement of the presumption of conformity is subject to the application of the edition of Standards as listed in Column 4 or, if no European Standard Edition exists, the International Standard Edition given in Column 2 of Table ZA.2.

WARNING 1 — Presumption of conformity stays valid only as long as a reference to this European Standard is maintained in the list published in the Official Journal of the European Union. Users of this standard should consult frequently the latest list published in the Official Journal of the European Union.

WARNING 2 — Other Union legislation may be applicable to the product(s) falling within the scope of this standard.

Contents

Page

Foreword	vi
Introduction	viii
1 Scope	1
2 Normative references	1
3 Terms, definitions, symbols and abbreviated terms	2
3.1 Terms and definitions	2
3.2 Symbols and abbreviated terms	10
4 Overview	12
4.1 Risk assessment and risk reduction process at the machine	12
4.2 Contribution to the risk reduction	14
4.3 Design process of an SRP/CS	14
4.4 Methodology	15
4.5 Required information	16
4.6 Safety function realization by using subsystems	17
5 Specification of safety functions	17
5.1 Identification and general description of the safety function	17
5.2 Safety requirements specification	18
5.2.1 General requirements	18
5.2.2 Requirements for specific safety functions	21
5.2.3 Minimizing motivation to defeat safety functions	24
5.2.4 Remote access	25
5.3 Determination of required performance level (PL _r) for each safety function	25
5.4 Review of the safety requirements specification (SRS)	26
5.5 Decomposition of SRP/CS into subsystems	26
6 Design considerations	27
6.1 Evaluation of the achieved performance level	27
6.1.1 General overview of performance level	27
6.1.2 Correlation between performance level (PL) and safety integrity level (SIL)	29
6.1.3 Architecture — Categories and their relation to MTTF _D of each channel, average diagnostic coverage and common cause failure (CCF)	29
6.1.4 Mean time to dangerous failure (MTTF _D)	36
6.1.5 Diagnostic coverage (DC)	37
6.1.6 Common cause failures (CCFs)	38
6.1.7 Systematic failures	38
6.1.8 Simplified procedure for estimating the performance level for subsystems	39
6.1.9 Alternative procedure to determine the performance level and PFH without MTTF _D	40
6.1.10 Fault consideration and fault exclusion	42
6.1.11 Well-tried component	43
6.2 Combination of subsystems to achieve an overall performance level of the safety function	43
6.2.1 General	43
6.2.2 Known PFH values	43
6.2.3 Unknown PFH values	44
6.3 Software based manual parameterization	44
6.3.1 General	44
6.3.2 Influences on safety-related parameters	45
6.3.3 Requirements for software based manual parameterization	46
6.3.4 Verification of the parameterization tool	47
6.3.5 Documentation of software based manual parameterization	47
7 Software safety requirements	47
7.1 General	47

7.2	Limited variability language (LVL) and full variability language (FVL)	49
7.2.1	Limited variability language (LVL)	49
7.2.2	Full variability language (FVL)	49
7.2.3	Decision for limited variability language (LVL) or full variability language (FVL)	49
7.3	Safety-related embedded software (SRESW)	51
7.3.1	Design of safety-related embedded software (SRESW)	51
7.3.2	Alternative procedures for non-accessible embedded software	52
7.4	Safety-related application software (SRASW)	52
8	Verification of the achieved performance level	55
9	Ergonomic aspects of design	55
10	Validation	55
10.1	Validation principles	55
10.1.1	General	55
10.1.2	Validation plan	57
10.1.3	Generic fault lists	58
10.1.4	Specific fault lists	58
10.1.5	Information for validation	58
10.2	Validation of the safety requirements specification (SRS)	59
10.3	Validation by analysis	60
10.3.1	General	60
10.3.2	Analysis techniques	60
10.4	Validation by testing	60
10.4.1	General	60
10.4.2	Measurement accuracy	61
10.4.3	Additional requirements for testing	62
10.4.4	Number of test samples	62
10.4.5	Testing methods	62
10.5	Validation of the safety functions	63
10.6	Validation of the safety integrity of the SRP/CS	63
10.6.1	Validation of subsystem(s)	63
10.6.2	Validation of measures against systematic failures	64
10.6.3	Validation of safety-related software	65
10.6.4	Validation of combination of subsystems	66
10.6.5	Overall validation of safety integrity	66
10.7	Validation of environmental requirements	66
10.8	Validation record	67
10.9	Validation maintenance requirements	67
11	Maintainability of SRP/CS	67
12	Technical documentation	68
13	Information for use	68
13.1	General	68
13.2	Information for SRP/CS integration	68
13.3	Information for user	69
Annex A (informative)	Guidance for the determination of required performance level (PL_r)	71
Annex B (informative)	Block method and safety-related block diagram	76
Annex C (informative)	Calculating or evaluating MTTF_D values for single components	78
Annex D (informative)	Simplified method for estimating MTTF_D for each channel	86
Annex E (informative)	Estimates for diagnostic coverage (DC) for functions and subsystems	88
Annex F (informative)	Method for quantification of measures against common cause failures (CCF)	92
Annex G (informative)	Systematic failure	96

Annex H (informative) Example of a combination of several subsystems	100
Annex I (informative) Examples for the simplified procedure to estimate the PL of subsystems	103
Annex J (informative) Example of SRESW realisation	111
Annex K (informative) Numerical representation of Figure 12	115
Annex L (informative) Electromagnetic interference (EMI) immunity	120
Annex M (informative) Additional information for safety requirements specification (SRS)	124
Annex N (informative) Avoiding systematic failure in software design	126
Annex O (informative) Safety-related values of components or parts of control systems	146
Bibliography	149

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

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.

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



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.

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, if a posts

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).

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 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

Table 1 (continued)

Symbol or abbreviated term	Description	Subclause or section
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 I
FVL	full variability language	3.1.40
FMEA	failure modes and effects analysis	6.1.5
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
n, N, Ñ	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 sub-systems	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

Table 1 (continued)

Symbol or abbreviated term	Description	Subclause or section
S, S1, S2	severity of injury	A.3.1
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

4 Overview

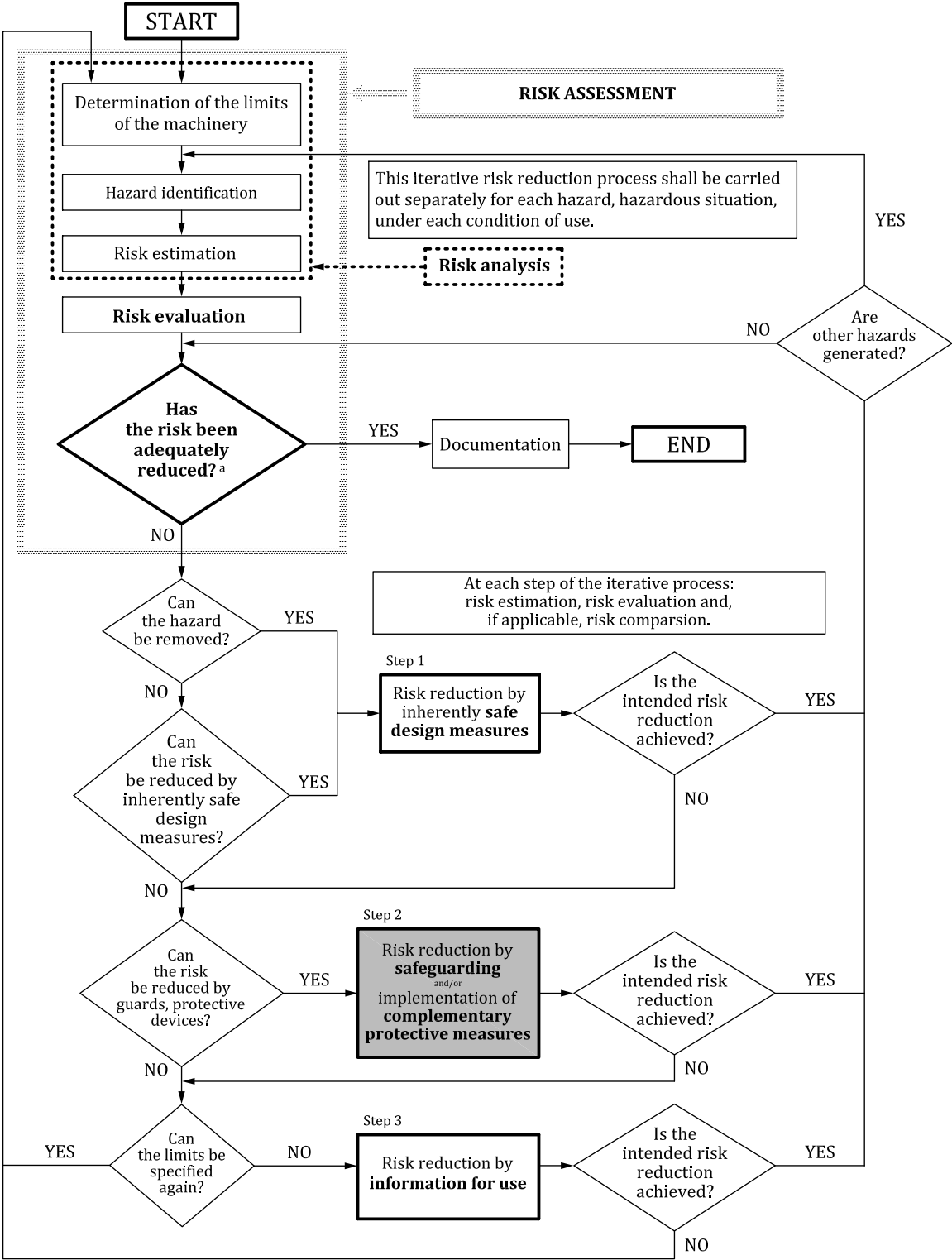
4.1 Risk assessment and risk reduction process at the machine

The risk assessment and risk reduction process is defined by ISO 12100:2010 as shown in [Figure 2](#). ISO 13849-1 (this document) is included in the risk reduction process when a safety function and its corresponding SRP/CS are used to provide the risk reduction.

NOTE 1 For further information see ISO/TR 22100-2:2013.

The SRS and the design of the SRP/CS shall take into account the result of the risk assessment including the intended use and reasonably foreseeable misuse of the machine (see [Figure 1](#) and [Figure 2](#)).

NOTE 2 This document does not apply to non-SRP/CS of a machine (see [Figure 6](#)).



Key

- ^a The first time the question is asked, it is answered by the result of the initial risk assessment.
-  Risk reduction by safeguarding may be realized by SRP/CS that execute safety functions. In this case this document can be applied.

NOTE Figure reproduced from ISO 12100:2010, Figure 1.

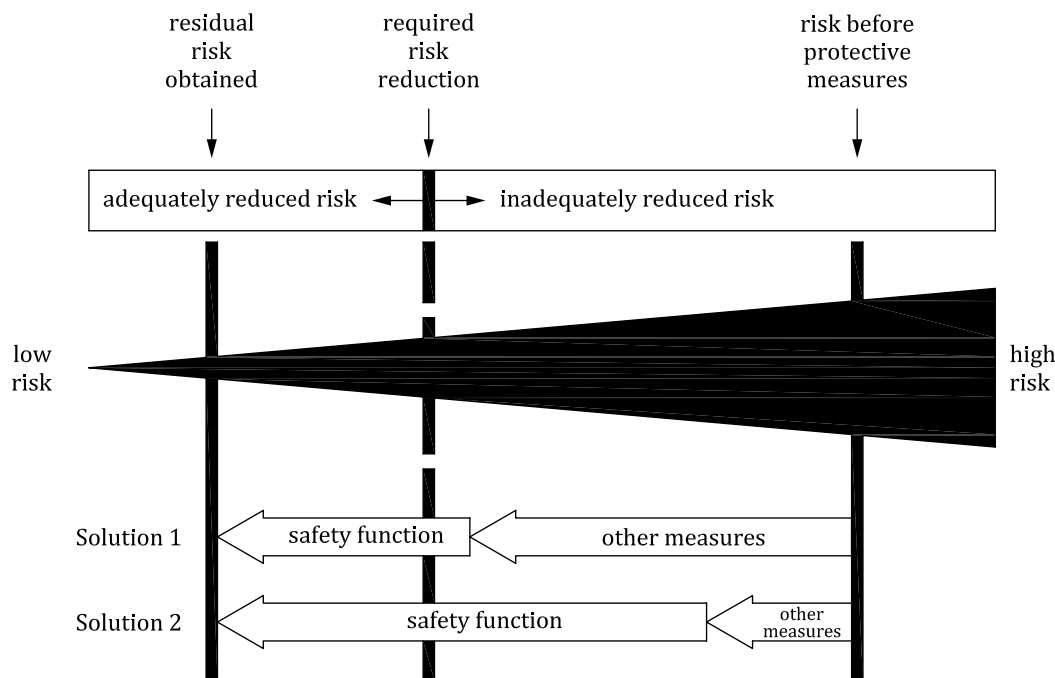
Figure 2 — Schematic representation of risk reduction process including iterative three-step method

NOTE 3 In special cases, this document applies also to step 3 of [Figure 2](#). For examples of indications and alarms see [Annex M](#).

4.2 Contribution to the risk reduction

From the risk assessment, the designer shall decide the contribution to the risk reduction provided by each relevant safety function carried out by the SRP/CS. This contribution covers the risk reduced by the application of each particular safety function (see [Figure 3](#)). It does not cover the overall risk of machinery under control.

EXAMPLE Safety-related stop function on a press initiated by using an electro-sensitive protective device or the door-locking safety function of a washing machine.



Key

- Solution 1 Important part of risk reduction due to protective measures other than the safety function (e.g. mechanical measures), small part of risk reduction due to safety function (e.g. guard or interlocking function).
- Solution 2 Important part of risk reduction due to the safety function, small part of risk reduction due to protective measures other than the safety function.

NOTE See ISO 12100:2010 for further information on risk reduction.

Figure 3 — Overview of the risk reduction measures for each hazardous situation

4.3 Design process of an SRP/CS

[Figure 4](#) shows the design process of an SRP/CS and determining whether the SRP/CS achieves the intended risk reduction.

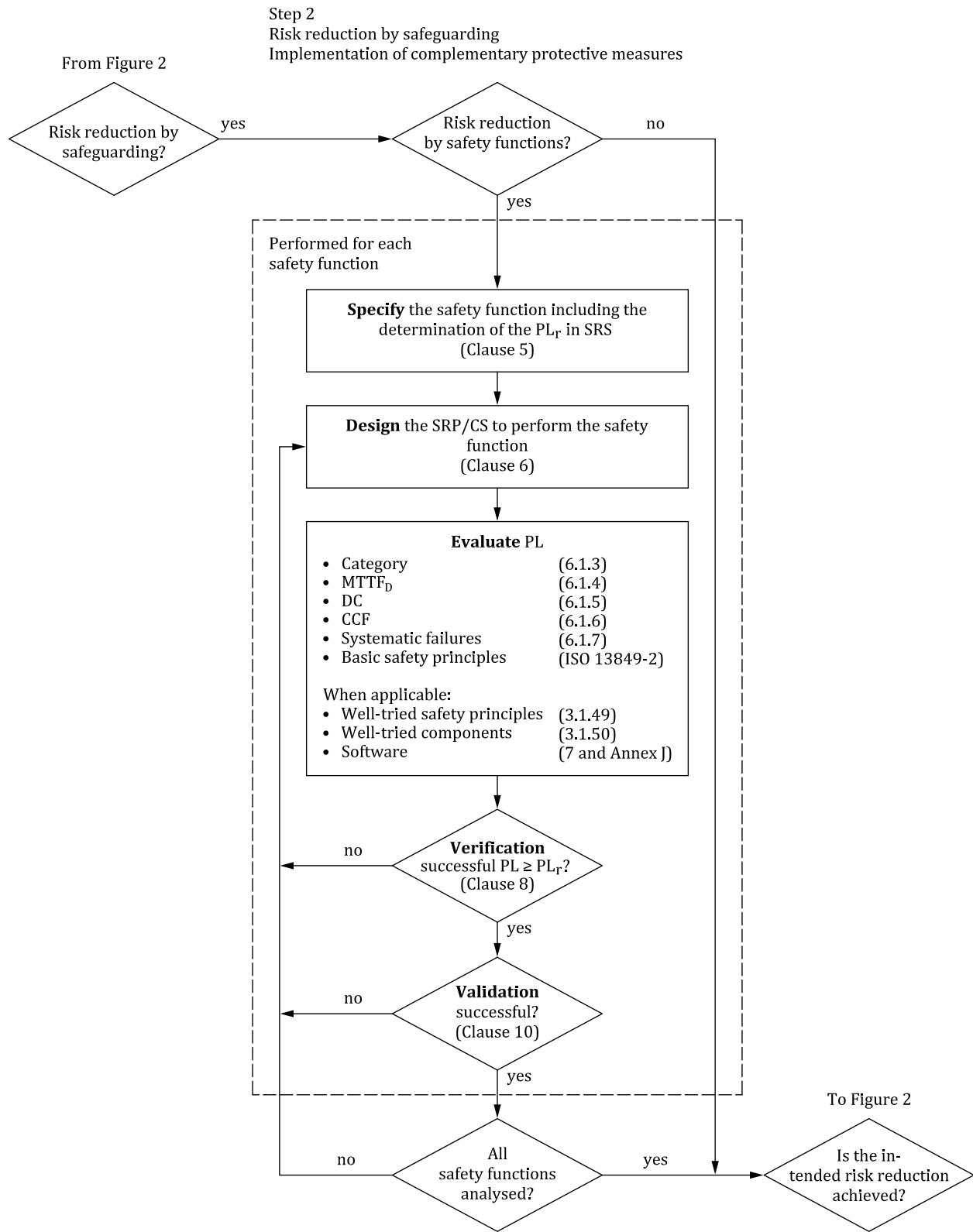


Figure 4 — Iterative process for design of safety-related parts of control systems (SRP/CS)

4.4 Methodology

This document uses the following methodology:

- a) specification of safety functions (Clause 5);

- b) design and technical realization of the safety functions including identification of the SRP/CSs and their subsystems which carry out each safety function;
 - 1) design considerations ([Clause 6](#)),
 - 2) software safety requirements ([Clause 7](#));
- c) verification that the achieved PL meets PL_r ([Clause 8](#));
- d) ergonomic aspects of the design ([Clause 9](#));
- e) validation ([Clause 10](#) or ISO 13849-2:2012);
- f) maintenance ([Clause 11](#));
- g) technical documentation ([Clause 12](#));
- h) information for use ([Clause 13](#)).

The required performance level (PL_r) corresponds to the required risk reduction to be provided by the safety function. The greater the contribution to the risk reduction needed (depending on the initial risk), the higher the required safety performance shall be. The performance levels of the safety function are defined in terms of average frequency of dangerous failure of the safety function per hour. There are five performance levels, ranging from providing a low contribution to risk reduction for PL a, to a high contribution to the risk reduction for PL e. The defined ranges of frequency of a dangerous failure per hour are shown in [Table 2](#).

Table 2 — Performance levels

PL	Average frequency of a dangerous failure per hour (PFH)
	1/h
a	$10^{-5} \leq \text{PFH} < 10^{-4}$
b	$3 \times 10^{-6} \leq \text{PFH} < 10^{-5}$
c	$10^{-6} \leq \text{PFH} < 3 \times 10^{-6}$
d	$10^{-7} \leq \text{PFH} < 10^{-6}$
e	$\text{PFH} < 10^{-7}$
NOTE The PFH value is considered to be identical to the PFH according to IEC 62061:2021 and the IEC 61508 series.	

Subsystems (see [5.5](#)) shall be evaluated using the same process as is used for SRP/CS systems, according to [Clauses 5](#) to [13](#). For each safety function, the achieved performance level shall meet or exceed the required performance level (PL_r).

4.5 Required information

To fulfil the requirements of this document, the following information is necessary:

- results of the risk assessment of the machine or part of it;
- information for all safety functions (see [Clause 5](#)) determined to be necessary for the risk reduction process for each hazard including:
 - detailed description of each safety function including their contribution to risk reduction (see [5.2](#));
 - determination of the required performance level (PL_r) for each safety function (see [5.3](#)).

NOTE This information can be given in applicable Type-C standards.

4.6 Safety function realization by using subsystems

The realisation of a safety function can be done by:

- using previously validated subsystems according to this document, IEC 62061:2021, the IEC 61508 series or other relevant safety-related product standards (e.g. the IEC 61496 series and IEC 61800-5-2);
- designing new subsystems according to this document; or
- a combination of both alternatives above (see example in [Figure 5](#)).

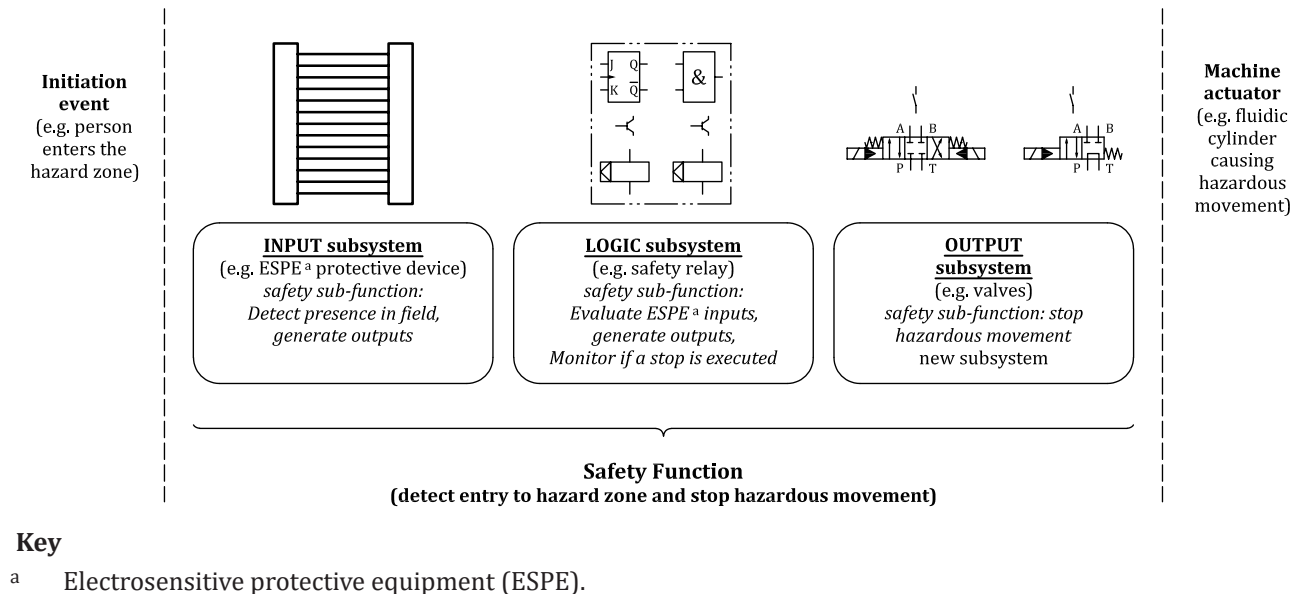


Figure 5 — Example of combination of subsystems

5 Specification of safety functions

5.1 Identification and general description of the safety function

A safety function shall have a general description to define how the SRP/CS contributes to risk reduction. The description shall be linked to hazards identified in the risk assessment and shall state how the function operates to achieve the required safety. The process for specifying safety functions requires detailed information from the risk assessment performed in accordance with ISO 12100:2010.

The objective of this subclause is to provide guidance on how to specify the requirements of each safety function to be implemented by the SRP/CS.

Part of the risk reduction process is to determine the safety functions of the machine, e.g. prevention of unexpected start-up. A safety function may be implemented by one or more subsystems combined as an SRP/CS, and several safety functions may share one or more subsystems, e.g. a logic unit, power control element(s).

Specification of the safety function can take place as described in ISO 12100:2010, 6.2.11 and afterwards as a part of the design specification for the SRP/CS according to this document.

[Clause 5](#) addresses the following steps:

- a) General description of the safety function (linking hazards to safety functions);
- b) Detailed description of the safety requirements (see [5.2](#));

- c) Determination of the PL_r for each safety function (see [5.3](#));
- d) Review of the SRS (see [5.4](#)).

5.2 Safety requirements specification

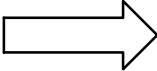
5.2.1 General requirements

5.2.1.1 General

The SRS is the basis for all SRP/CS design activities and shall document details of each safety function to be performed.

The SRS provides the necessary information at the transition from the risk assessment and risk reduction process according to ISO 12100:2010 to the SRP/CS design and evaluation process according to this document, especially if these two processes are performed by different persons or organizations (see [Table 3](#)).

Table 3 — Transition from the risk assessment and risk reduction process according to ISO 12100:2010 to the SRP/CS design and evaluation process according to ISO 13849-1 (this document)

Necessary information to produce the SRS (see 5.2.1.2)	Transformation	Examples of specifications of safety functions in the SRS (see 5.2.1.3)
— results of risk assessment of the machine or part of it, including hazardous parts and required overall risk reduction — machine operating characteristics, e.g. intended use — emergency operation — description of the interaction of different working processes and manual activities, e.g. repairing — ergonomic aspects — limits of use in relation to environmental conditions		required safety functions (examples): 1) interlocking function — operating mode (all) — triggering event: opening of a movable guard — safety-related reaction: safe torque off (STO) of all movements — PL_{r d} — response time — etc. 2) safely limited speed (SLS) — operating mode (manual) — triggering event: speed is higher than the specified limit — safety-related reaction: safe torque off (STO) of all movements — PL_{r c} — response time — etc.

5.2.1.2 Necessary information to produce the safety requirements specification (SRS)

NOTE 1 The following information is used for technical documentation. For information for users see 13.3.

The following information shall be available to the designer of the safety-related control system to develop the SRS where relevant:

- a) results of the risk assessment of the machine or part of it for each specific hazard where the associated risk reduction measure(s) relies on a safety-related control system to perform a safety function;
- b) machine operating characteristics, including:
 - 1) intended use of the machine,
 - 2) reasonably foreseeable misuse,
 - 3) operating modes (e.g. local mode, automatic mode, modes related to a zone or part of the machine),
 - 4) the mode(s) of operation during which the safety function is to be active,

- 5) cycle time, and
- 6) response time until a safe state is achieved according to ISO 13855:2010, 5.1;

NOTE 2 The response time of the control system is part of the overall response time of the machine. The required overall response time of the machine can influence the design of the safety-related part, e.g. the need to provide a braking system.

NOTE 3 Operational functions (e.g. starting, normal stopping) can also be safety functions, but this can be ascertained only after a complete risk assessment on the machinery has been carried out.

- c) emergency operation (IEC 60204-1:2016+AMD1:2021, Annex E);
- d) description of the interaction of different working processes and manual activities (e.g. repairing, setting, cleaning, trouble shooting, modes of operation with the safeguards suspended);
- e) ergonomic aspects to minimize incorrect operation or defeating;
- f) limits of use in relation to environmental conditions;
- g) effect of overlapping hazards (see [A.4](#)).

5.2.1.3 Specification of all safety functions in the safety requirements specification (SRS)

The SRS shall have the following information for each safety function in relation to the specific application:

- a) the brief description / title of the safety function;
- b) the event that triggers the safety function;
- c) the reaction to be initiated by the safety function output(s) to reach the intended safe state;
EXAMPLE 1 Stop hazardous movements.
- d) the required performance level PL_r (see [5.3](#));
- e) the response time for the machine to achieve a safe state after the demand is made upon the safety function, e.g. the overall system stopping performance (reaction time plus stopping time) according to ISO 13855:2010;
- f) the operating mode(s) during which the safety function is to be active;
- g) interfaces of the safety function with the machine control system and other safety functions;
- h) if needed, in case of a fault detection in a functional channel, procedures to bring the machine to a safe state including how the safe state is maintained until the fault is repaired;

EXAMPLE 2 If there is a fault in a functional channel and a controlled stop is not possible, then a fault reaction can be initiated by using an immediate, uncontrolled stop.

- i) the behaviour of the machine on the loss of power (see [5.2.2.8](#));

EXAMPLE 3 It can be necessary to hold a vertical axis in position to prevent a fall due to gravity forces. Where external forces can have an impact on functional safety, for instance on those gravity loaded axes, a reinforcement (e.g. for power elements) can be necessary because of systematic requirements. An appropriate design solution can be the integration of a non-return valve on cylinders or supplementary mechanical brakes. This can also require the design of two separate safety functions: One with power available and another without power available.

- j) the demand rate of the safety function and/or the frequency of operation of the SRP/CS;
- k) the priority of the safety functions that can be simultaneously active and that can cause conflicting action;

EXAMPLE 4 An emergency stop function has priority over all other functions.

EXAMPLE 5 The safely limited speed (SLS) function can be a precondition of a "hold to run" safety function.

- l) safety-requirements of type-C standards for the design of an SRP/CS or subsystem (e.g. ISO 23125:2015, ISO 16090-1);
- m) the conditions to permit the restart after the activation of the safety function.

NOTE Automatic reset of a safety function is appropriate in situations where continuous detection of an individual prevents the hazardous situation.

See [5.2.2](#) and [Annex M](#) for typical safety functions and their characteristics and safety-related parameters.

5.2.2 Requirements for specific safety functions

5.2.2.1 General

This subclause provides additional requirements for specific safety functions that are commonly applied in many SRP/CS.

5.2.2.2 Safety-related stop function

A safety-related stop function (e.g. initiated by a safeguard) shall as soon as necessary after actuation, put the machine in a safe state. Such a safety-related stop function shall have priority over all relevant starts and non-safety-related stops. When a group of machines is working together in a coordinated manner, provision shall be made for signalling either the supervisory control or the other machines, or both, that such a stop condition exists.

As a result of the risk assessment, safety-related stop functions can be realised according to the stop categories in IEC 60204-1:2016+AMD1:2021, 9.2.2.

NOTE IEC 61800-5-2:2016 provides information about safety-related power drive systems including descriptions of safe-torque off (STO), safe stop 1 (SS1), safe stop 2 (SS2) and safe operating stop (SOS).

After a stop command has been initiated by a safety function, the stop condition shall be maintained until safe conditions for restarting exist. See also [Table M.1](#).

5.2.2.3 Manual reset function

The re-establishment of the safety function by resetting of the safeguard cancels the stop command. If indicated by the risk assessment, this cancellation of the stop command shall be confirmed by a manual, separate and intended action (manual reset).

The manual reset function shall:

- be provided through a separate and manually operated device that is separate from start command,
- only be achieved if all affected safety functions and safeguards are operational,
- not initiate a hazardous situation by itself,
- be initiated by intended action,
- enable the control system to accept a separate start command, and
- only be accepted by monitored signal change, in order to avoid foreseeable misuse.

When the function “manual reset” is required to be a safety function (e.g. prevention of unexpected start-up), the required performance level (PL_r) shall be determined. The PL of the manual reset function can be different from the PL_r of the associated safety function.

NOTE The manual reset function often is not a separate additional safety function when the safe state is still maintained by a safety function (safe condition), e.g. initiated by a safeguard (cover) where stepping behind is not possible.

The reset actuator shall be located outside the hazard zone and in a position from which there is sufficient visibility to ensure that no person is inside the hazard zone. It shall not be possible to activate the reset function from inside the hazard zone. Where the visibility of the hazard zone is not sufficient, a specific reset sequence or monitoring of the area that is not visible, shall be provided. When specific reset sequence or monitoring of the area are not possible, other equivalent risk reduction measures shall be used.

EXAMPLE One solution is the use of a sequenced resetting. The reset function is initiated within the hazard zone by the first actuator in combination with a second reset actuator located outside the hazard zone (near the safeguard). This reset procedure can be realized within a limited time before the control system accepts a separate start command. Monitoring of the area can be done by, e.g. use of presence sensing devices that detect persons in hazard zones not visible from the reset position.

See also [Table M.1](#).

5.2.2.4 Restart function

A restart shall take place automatically only if the safe condition is guaranteed. In particular, for interlocking guards with a start function, ISO 12100:2010, 6.3.3.2.5 shall apply.

EXAMPLE In automatic machine operations, sensor feedback signals to the control system are often used to control the process flow. If a workpiece has come out of position, the process flow is stopped. If the monitoring of the interlocked safeguard does not have a higher priority than the automatic process control, there can be a danger of unexpected restarting of the machine while the operator readjusts the workpiece. Therefore, the automatic restart should not be allowed until the safeguard is closed again and the operator has left the hazard zone. The contribution of the prevention of unexpected start-up (see ISO 14118:2017) provided by the control system is dependent on the result of the risk assessment.

See also [Table M.1](#).

5.2.2.5 Local control function

When a machine is controlled locally, e.g. by a portable control station that can be a portable device or pendant, the following requirements shall apply:

- the means for granting local control shall be situated outside the hazard zone;
- it shall only be possible to initiate command by a local control station in a zone defined by the risk assessment in order to avoid hazardous situations;
- switching between local and a different control shall not create a hazardous situation;
- initiation of commands from multiple control stations (local or remote) shall not lead to a hazardous situation. It can be necessary to preclude use of other control stations when a local control station is selected or when certain commands are initiated.

See also [Table M.1](#).

5.2.2.6 Muting function

Muting is a temporary automatic suspension of a safety function by the machine safety-related control system. It can be used to allow access by persons or by materials:

- during a non-hazardous portion of the machine cycle, or

— when safety is maintained by other means.

The muting function shall be initiated and terminated automatically. This shall be achieved by the use of appropriately selected and placed sensors or by signals from the machine control system. Incorrect signals, sequence, or timing of the muting sensors or signals shall not allow a mute condition.

The part or parts of the control system that performs the muting function shall have an appropriate safety-related performance (PL according to this document or SIL according to IEC 62061:2021) and shall not reduce the safety-related performance of the protective function below that required for the application.

At the end of muting, all affected safety functions shall be reinstated and active.

The implementation of muting shall meet the requirements of IEC 62046:2018. See also [Table M.1](#).

5.2.2.7 Safety-related parameters

When safety-related parameters, e.g. position, speed, temperature, time, torque or pressure, deviate from pre-set limits, the safety-related control system shall initiate appropriate measures.

If errors in manual inputting of safety-related data in programmable or configurable electronic systems can lead to a hazardous situation, then a data checking measure shall be provided, e.g. check of limits, either format or logic input values, or both. For additional requirements, see [6.3](#) and [Table M.2](#).

5.2.2.8 Fluctuations, loss and restoration of power sources

When fluctuations in energy levels outside the designed operating range occur, including loss of energy supply, the SRP/CS shall continue to provide or initiate output signal(s) which will enable other parts of the machine system to maintain a safe state. See also [Table M.2](#).

5.2.2.9 Requirements for operating mode selection

Selection of operating mode is a safety function when the selection enables or disables safety function(s). The following is required:

- a) only one operating mode shall be active at a time; each selected operating mode shall be clearly identifiable or indicated;
- b) mode selection by itself shall not initiate machine operation. A separate actuation of the start control shall be required;
- c) when changing from one operating mode to another, safety functions and/or risk reduction measures necessary for the selected operating mode shall be activated without any loss of the intended risk reduction during the transition;
- d) the means of selecting the operating mode shall not degrade the PL of the safety functions active in that mode.

See also [Table M.1](#).

5.2.2.10 Safety function(s) for maintenance tasks

The design of the machine shall take into account maintenance tasks on the machine and provide safety functions for these tasks. The results of the risk assessment for each maintenance task shall be considered in the specification of the safety functions.

NOTE 1 Maintenance tasks can include, but are not limited to:

- setting;
- teaching/programming;

- process/tool changeover;
- cleaning and housekeeping;
- sanitizing;
- planned or unplanned preventive or corrective maintenance;
- troubleshooting/fault finding;
- fault diagnosis.

Some maintenance tasks require a full isolation of the machine from all power sources and therefore do not rely on the SRP/CS. Where manual suspension or override of specific safety functions is needed for maintenance tasks that require either power or machine movements, or both, while maintenance personnel are inside the hazard zone, such operation shall only be allowed by providing appropriate alternative safety functions (e.g. enabling device safety function with a speed limiting safety function).

EXAMPLE Teaching/ programming, troubleshooting, process fine-tuning are tasks requiring power and machine movement.

The following safety functions, used singularly or in combination, are examples of what is often provided for maintenance tasks:

- a) hold-to-run;
- b) enabling control;
- c) monitoring or limiting of, e.g. speed, torque, power, position, location, temperature, level;
- d) prevention of unexpected start-up;
- e) disconnection and energy dissipation;
- f) mechanical restraint or containment.

See [Annex M](#) for additional information.

The motivation to defeat or circumvent risk reduction measures provided by the SRP/CS during maintenance of the machine shall be considered when specifying, designing and selecting the SRP/CS (see [5.2.3](#)).

The design of SRP/CS shall consider that additional personnel other than the intended operator(s) perform a task, e.g.:

- an operator performs reset and restart functions while maintenance personnel are inside the hazard zone;
- risk reduction measures intended to protect an individual are inappropriately used for multiple personnel.

In maintenance mode, the design of the SRP/CS shall prevent a remote access (see [5.2.4](#)) to the machine control system without appropriate notification or indication to persons that are at or near the machine.

5.2.3 Minimizing motivation to defeat safety functions

The motivation to defeat or circumvent a safety function depends on the process, the intended use of the machine (or parts of the machine) and the design details of the risk reduction measure(s). The motivation to defeat a safety function shall be minimized in the design of the SRP/CS.

NOTE 1 Safety research has shown that many injuries occur due to defeat of either safety function or safeguards, or both. See Bibliography for more information.

EXAMPLE When designing risk reduction measures and safety functions, the following circumstances can introduce a motivation to defeat and can be considered:

- the risk reduction measure prevents the task from being performed;
- there is a need to perform a task that was not identified and assessed for hazards and risks;
- the risk reduction measure slows down production or interferes with any other activities or preferences of the user;
- the risk reduction measure is difficult to use;
- either the risk reduction measure or its associated hazard, or both, are not recognized as such by personnel;
- the risk reduction measure is not accepted as suitable, necessary or appropriate for its function;
- unlimited access to the SRP/CS hardware and software systems which implement the safety functions.

NOTE 2 Providing means to perform tasks easily whilst protecting operators can lessen the motivation to defeat or circumvent safety function(s) and/or safeguard(s).

NOTE 3 ISO 14119 gives a method and shows examples on how to minimize possibilities to defeat an interlocking device.

The use and access to programmable systems introduces an additional possibility to defeat or circumvent safety functions if not properly applied or supervised.

5.2.4 Remote access

When the machine control system can be accessed remotely, the SRP/CS shall remain operational. Additional risk reduction measures can be used when provided in the information for use.

The design of the SRP/CS shall only allow remote access of a machine when specific measures are in place to prevent dangerous situations that can arise due to the undetected presence of persons being inside or near to the machine (e.g. see [5.2.2.2](#)).

Safety-related software of the SRP/CS shall not be modifiable by remote access unless the local validation of the safety function is performed.

NOTE A remote start that is unexpected to persons working at the machine can lead to injury.

5.3 Determination of required performance level (PL_r) for each safety function

For each selected safety function, a required performance level (PL_r) shall be determined and documented. The determination of the PL_r shall be based on the result of the risk assessment and shall correlate to the needed risk reduction (see [Figure 3](#)). [Annex A](#) provides guidance for the determination of the PL_r for the safety function. Overlapping hazards, if relevant, shall also be considered when defining the safety functions. See [A.3](#) for further guidance.

NOTE 1 Other methods for the determination of PL_r can be used (e.g. the method in IEC 62061:2021, Annex A).

NOTE 2 Type-C standards typically provide information on PL_r.

NOTE 3 As the methodology for determining PL_r includes subjective estimations, some variability is acceptable in the practical application of particular cases.

NOTE 4 The PL_r for a safety function determines the required reliability of the control system to execute the safety function and to achieve the intended risk reduction. The PL_r is determined using several factors of risk. See also [Annex A](#).

5.4 Review of the safety requirements specification (SRS)

The SRS shall be verified against the risk assessment before starting the design. The review shall ensure that all safety functions are specified to achieve the intended risk reduction at the machine. See also [10.2](#) for the validation of the SRS.

The SRS shall be validated according to the requirements of [10.1.1](#)

5.5 Decomposition of SRP/CS into subsystems

The safety functions can be decomposed into sub-functions that are allocated to subsystems. The description of each sub-function shall include:

- the safety requirements for the sub-function (functional and integrity);
- inputs and outputs of each sub-function.

An SRP/CS can comprise:

- one or several previously validated subsystem(s);
- one or several subsystem(s) based on subsystem element(s);
- a combination of both alternatives above.

By definition of the subsystem, a dangerous failure of any subsystem results in the loss of the whole safety function.

EXAMPLE [Figure 6](#) provides an example of decomposition starting with a detection and evaluation of an 'initiating event' (e.g. manual actuation of a push button, opening of guard, interruption of beam of AOPD) and ending with an output causing a safe reaction of a 'machine actuator' (e.g. motor, cylinder).

NOTE 1 Safety function 1 is decomposed into sub-function 1, sub-function 2 and sub-function 3. Sub-function 1 is performed by subsystem 1, etc.

NOTE 2 Safety function 2 is decomposed into sub-function 4 and sub-function 5. Sub-function 4 is performed by subsystem 4, etc.

NOTE 3 Safety function 3 is decomposed into sub-function 6 and sub-function 5. Sub-function 6 is performed by subsystem 6, etc.

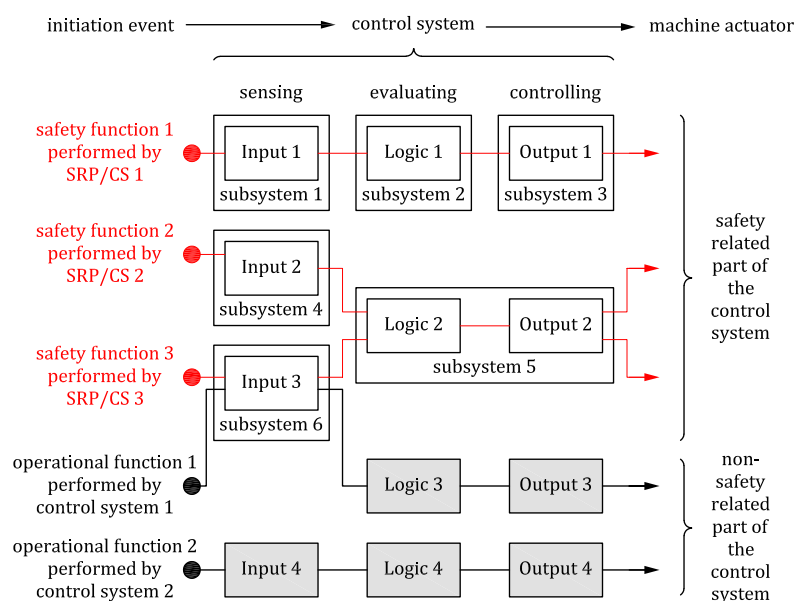


Figure 6 — Example of decomposition of safety functions and their allocation to subsystems

[Figure 6](#) shows a block diagram of subsystems combined as SRP/CS(s) for:

- initiation event (e.g. opening of a guard, interruption of beam of AOPD);
- input (e.g. limit switch, sensor, AOPD) (subsystems 1, 4 and 6);
- logic/processing (subsystems 2 and 5);
- output/power control elements (e.g. valve, contactor, current converter, brakes) (subsystems 3 and 5);
- machine actuator (e. g. motor, cylinder);
- interconnecting means (e.g. electrical, optical).

The decomposition of an SRP/CS into subsystems represented in [Figure 6](#) is typical, but the whole SRP/CS may be also realized by a single subsystem or more than three subsystems.

NOTE 4 An SRP/CS can be implemented by one single subsystem having a sensor, logic and power control elements. An example for an SRP/CS implementation with a single subsystem is an “Intelligent” sensor unit (e.g. light curtain, laser scanner) with integrated output switching device (e.g. relay to switch-off a dangerous movement).

NOTE 5 One subsystem or SRP/CS can implement safety functions and standard control functions. The designer can use any of the technologies available, single or in combination. SRP/CS can also provide an operational function (e.g. an AOPD as a means of cycle initiation).

The designer of a previously validated subsystem shall provide the relevant information according to [13.2](#).

NOTE 6 The designer of a previously validated subsystem can be a system integrator, machine manufacturer or a component manufacturer.

6 Design considerations

6.1 Evaluation of the achieved performance level

6.1.1 General overview of performance level

The ability to perform a safety function is determined by the evaluation of the performance level.

A performance level shall be determined for either each subsystem or each combination of subsystems, or both, that perform a safety function. The PL of the subsystem shall be determined by the estimation of the following aspects:

- a) the architecture (see [6.1.3](#));
 - 1) assign a category to the subsystem;
 - 2) evaluate if the applicable qualitative (non-quantifiable) requirements of the category are met, including:
 - basic safety principles (ISO 13849-2:2012, Tables A.1, B.1, C.1 and D.1);
 - well-tried safety principles (ISO 13849-2:2012, Tables A.2, B.2, C.2 and D.2);
 - well-tried components (ISO 13849-2:2012, Tables A.3 and D.3, Annexes B and C);
 - 3) evaluate that required behaviour under fault condition(s) is met;
- b) the $MTTF_D$ value for single components (see [6.1.4](#), and [Annexes C](#) and [D](#));

- c) the DC (see [6.1.5](#) and [Annex E](#));
- d) the CCF (see [6.1.6](#) and [Annex F](#));
- e) the effect of the safety-related software design on the operation of the hardware (see [Clause 7](#) and [Annex J](#));
- f) the effect of measures against systematic failures (see [6.1.7](#) and [Annex G](#)).

NOTE 1 Other parameters, e.g. operational aspects, demand rate, test rate, can have a particular influence.

NOTE 2 For safety-related values of components or parts of control systems see [Annex O](#).

These aspects can be grouped under two approaches in relation to the evaluation process:

- quantifiable aspects (MTTF_D value for single components, DC, CCF, architecture);
- non-quantifiable, qualitative aspects which affect the behaviour of the subsystem (behaviour of the safety function under fault conditions, safety-related software, systematic failure, the application of basic and well-tried safety principles, the use of well-tried components, environmental conditions and fault exclusion).

NOTE 3 The contribution of reliability (e.g. MTTF_D, architecture) can vary with the SRP/CS used.

NOTE 4 There are several methods for estimating the quantifiable aspects of the PL for any type of system (e.g. a complex structure), for example, Markov modelling, generalized stochastic petri nets (GSPN), reliability block diagrams (see, e.g. the IEC 61508 series, IEC 61078, the IEC 62021 series).

To make the assessment of the PL easier, this document provides a simplified method based on the definition of five designated architectures that fulfil specific design criteria and behaviour under a fault condition (see [6.1.3](#)).

For PL evaluation of a subsystem the requirements are given in [6.1](#). A simplified approach for the PL evaluation of a subsystem is given in [6.1.8](#) ([Figure 12](#)) and [6.1.9](#), using the procedure given in [Annexes B](#) to [Annex H](#), [Annex J](#), [Annex K](#) and [Annex L](#). For PL evaluation of subsystem combinations see [6.2](#).

Qualitative aspects of the PL and the avoidance of systematic failures shall be achieved by fulfilling the requirements and guidance of this document. See [6.1.7](#) for systematic failure and guidance in [Annex G](#).

Where product-specific standards such as the IEC 61496 series for electro-sensitive protective equipment (ESPE) or the ISO 13856 series for pressure-sensitive protective equipment, specify requirements to avoid or control systematic or random failures, such subsystems shall meet the requirements of these product standards in addition to the requirements specified in this document.

Risk reduction measures shall be applied and the following shall be fulfilled:

- Reduce the probability of faults at the component level which affect the safety function. This can be done by increasing the reliability of components, e.g. by selection of either well-tried components or applying well-tried safety principles, or both, in order to minimize or exclude critical faults or failures (see also ISO 13849-2:2012).
- Improve the architecture of the subsystem to avoid the dangerous effect of a fault. Some faults can require detection, thereby necessitating an either redundant or monitored architecture, or both.

Reducing the probability of faults and avoiding dangerous effects of faults can be applied separately or in combination. Depending on the technologies, this can be achieved by

- selecting reliable components and by fault exclusions; or
- the safety function having either a redundant or monitored architecture system, or both.

The structure including fault tolerance and fault detection are important parameters to determine the PL. Architectural constraints limit the maximum achievable PL of category B, 1 and 2. For these architectural constraints, see [6.1.3.2.2](#) to [6.1.3.2.4](#).

Requirements to prevent or avoid CCFs shall be fulfilled.

For subsystems that have PL or SIL and PFH values from the manufacturer, further estimation (e.g. DC, MTTF_D, CCF, SRESW evaluation) is unnecessary. See also [Table 0.1](#).

6.1.2 Correlation between performance level (PL) and safety integrity level (SIL)

When a safety function is designed using one or more subsystems, each subsystem shall be designed either using PLs according to this document, or using SILs according to IEC 62061:2021 or the IEC 61508 series. Subsystems designed according to the IEC 61508 series or IEC 62061:2021 may be used but shall be restricted to those designed for high demand or continuous mode that use Route 1_H (see IEC 61508-2:2010, 7.4.4.2). Subsystems shall be combined according to [6.2](#). See [Table 4](#) for correlations between PLs and SILs.

Table 4 — Correlation between performance level (PL) and safety integrity level (SIL)

PL	SIL (see IEC 62061:2021 for information) high/continuous operating mode
a	no correlation
b	1
c	1
d	2
e	3

NOTE 1 PL a has no correlation on the SIL scale and is mainly used to reduce the risk of slight, normally reversible, injury.

NOTE 2 PL e corresponds to SIL 3 which is defined as the highest level typically used for machinery.

6.1.3 Architecture — Categories and their relation to MTTF_D of each channel, average diagnostic coverage and common cause failure (CCF)

6.1.3.1 General

Subsystems designed according to this document shall be in accordance with the requirements of one of the categories specified in [6.1.3.2](#). The categories are fundamental to achieving a specific PL. They describe the required behaviour of the subsystem in respect to its resistance to faults based on the design considerations described in [6.1.1](#).

Category B is the basic category. The occurrence of a fault can lead to the loss of the safety function. In category 1, improved resistance to faults is achieved predominantly by using high quality components. In categories 2, 3 and 4, improved performance is achieved predominantly by improving either fault tolerance or diagnostic measures, or both. In category 2 this is provided by periodically checking that the specified sub-function is being performed correctly (without faults). In categories 3 and 4, this is provided by ensuring that the single fault does not lead to the loss of the sub-function. In category 4, and whenever reasonably practicable in category 3, such faults are detected. Category 4 is resistant to accumulation of faults. [Table 5](#) gives an overview of categories of the subsystem, the requirements and the sub-function behaviour in case of faults.

When considering the causes of failures in some components it is possible to exclude certain faults (see [6.1.10.3](#)).

Table 5 — Overview of requirements for categories

Category	Summary of requirements for subsystems	Sub-function behaviour	Principle used to achieve safety	MTTF _D of each functional channel	DC _{avg}	CCF
B (see 6.1.3.2.2)	Either subsystems or their protective equipment, or both, as well as their components, shall be designed, constructed, selected, assembled and combined in accordance with relevant standards so that they can withstand the expected influences. Basic safety principles shall be used.	The occurrence of a fault can lead to the loss of the sub-function.	Mainly characterized by selection of components	Low to medium	None	Not relevant
1 (see 6.1.3.2.3)	Requirements of B shall apply. Well-trying components and well-trying safety principles shall be used.	The occurrence of a fault can lead to the loss of the sub-function, but the probability of occurrence is lower than for category B.	Mainly characterized by selection of components	High	None	Not relevant
2 (see 6.1.3.2.4)	Requirements of B and the use of well-trying safety principles shall apply. Subsystems shall be tested at suitable intervals.	The occurrence of a fault can lead to the loss of the sub-function between the tests. The loss of sub-function is detected by the test.	Mainly characterized by structure	Low to high	Low to medium	See Annex F
3 (see 6.1.3.2.5)	Requirements of B and the use of well-trying safety principles shall apply. Subsystem shall be designed, so that — a single fault in any of these parts does not lead to the loss of the sub-function, and — whenever reasonably practicable, the single fault is detected.	When a single fault occurs, the sub-function is always performed. Some, but not all, faults will be detected. Accumulation of undetected faults can lead to the loss of the sub-function.	Mainly characterized by structure (redundancy)	Low to high	Low to medium	See Annex F
NOTE For full requirements, see 6.1.3.2 .						

Table 5 (continued)

Category	Summary of requirements for subsystems	Sub-function behaviour	Principle used to achieve safety	MTTF _D of each functional channel	DC _{avg}	CCF
4 (see 6.1.3.2.6)	Requirements of B and the use of well-tried safety principles shall apply. Subsystem shall be designed, so that — a single fault in any of these parts does not lead to a loss of the sub-function, and — the single fault is detected at or before the next demand upon the sub-function, but if this detection is not possible, an accumulation of undetected faults shall not lead to the loss of the sub-function.	When a single fault occurs, the sub-function is always performed. Detection of accumulated faults reduces the probability of the loss of the sub-function (high DC). The faults will be detected in time to prevent the loss of the sub-function.	Mainly characterized by structure (redundancy)	High	High including accumulation of faults	See Annex F
NOTE For full requirements, see 6.1.3.2 .						

The selection of a category for a particular subsystem depends mainly upon

- a) the reduction in risk to be achieved by the safety function to which the subsystem contributes,
- b) the required performance level (PL_r),
- c) the technologies used,
- d) the consequences arising in the case of a fault(s) in an element of the subsystem,
- e) the possibilities of avoiding a fault(s) in that subsystem (systematic failure),
- f) the mean time to dangerous failure (MTTF_D),
- g) the diagnostic coverage (DC), and
- h) the CCFs in the case of categories 2, 3 and 4.

6.1.3.2 Designated architectures — Specification of categories

6.1.3.2.1 General

The following designated architectures meet the requirements of the respective category.

The designated architectures show a logical representation of the structure of the subsystems for each category.

NOTE 1 For categories 3 and 4 not all parts are necessarily physically redundant but there are redundant means of assuring that a single fault cannot lead to the loss of the sub-function. Therefore, the technical realization (for example, the circuit diagram) can differ from the logical representation of the architecture.

[Figure 7](#) to [Figure 11](#) do not show examples but general designated architectures. A deviation from these architectures is always possible, but any deviation shall be justified, by means of appropriate

analytical tools, e.g. Markov modelling, fault tree analysis (FTA), such that the subsystem meets the required performance level (PL_r). For a subsystem that deviates from the designated architectures, a detailed calculation shall be provided to demonstrate the achievement of the PL_r .

The lines and arrows in [Figure 7](#) to [Figure 11](#) represent logical interconnecting means and, where applicable, diagnostic means.

NOTE 2 The structure of a subsystem is a key characteristic having great influence on the PL. Even if the variety of possible structures is high, the basic concepts are often similar. Thus, most structures that are present in the machinery field can be mapped to one of the categories. For each category, a typical representation as a safety-related block diagram can be made. These typical realizations are called designated architectures and are listed in the context of each of the following categories.

If the simplified procedure of [6.1.8](#) is used to estimate the PL, the architecture of the subsystem shall be equivalent to the designated architecture of the claimed category.

6.1.3.2.2 Category B

Subsystem of category B shall, as a minimum, be designed, constructed, selected, assembled and combined in accordance with the relevant standards and use basic safety principles (see also ISO 13849-2:2012) for the specific application to withstand

- the expected operating stresses, e.g. the reliability with respect to breaking capacity and frequency,
- the influence of the processed material, e.g. detergents in a washing machine, and
- other relevant external influences, e.g. mechanical vibration, electromagnetic interference (EMI), power supply interruptions or disturbances.

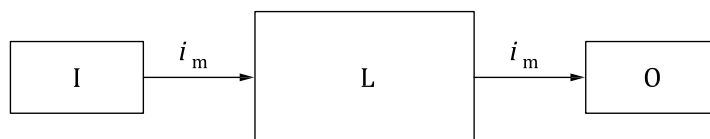
The $MTTF_D$ of the channel shall be at least low.

The maximum PL achievable with category B is PL b.

NOTE 1 There is no average diagnostic coverage ($DC_{avg} = \text{none}$) within category B architectures. In such structures, the consideration of CCF is not relevant.

NOTE 2 When a fault occurs it can lead to the loss of the sub-function.

Specific requirements for EMI (immunity requirements) are found in the relevant product or generic standards. Immunity requirements are particularly relevant for subsystems. Subsystems containing active electronic components shall meet EMI immunity requirements based on the environment as appropriate. For practical guidance see [Annex L](#).



Key

- i_m interconnecting means
- I input device, e.g. sensor
- L logic
- O output device, e.g. main contactor

Figure 7 — Designated architecture for category B

6.1.3.2.3 Category 1

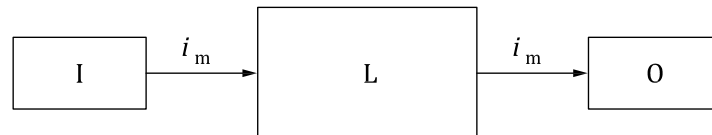
For category 1, the same requirements as those according to [6.1.3.2.2](#) for category B shall apply. In addition, the following applies.

Subsystems of category 1 shall be designed and constructed using well-trying components according to 6.1.11 and well-trying safety principles (see 3.1.49 and ISO 13849-2:2012). The $MTTF_D$ of the channel shall be high.

NOTE 1 There is no average diagnostic coverage ($DC_{avg} = \text{none}$) within category 1 architectures. In such structures (single-channel architectures) the consideration of CCF is not relevant.

The maximum PL achievable with category 1 is PL c.

NOTE 2 When a fault occurs it can lead to the loss of the safety function. However, the $MTTF_D$ of the single channel in category 1 is higher than in category B. Consequently, the loss of the safety function is less likely.



Key

- i_m interconnecting means
- I input device, e.g. sensor
- L logic
- O output device, e.g. main contactor

Figure 8 — Designated architecture for category 1

6.1.3.2.4 Category 2

For category 2, the same requirements as those according to 6.1.3.2.2 for category B shall apply. “Well-trying safety principles” according to 3.1.49 and ISO 13849-2:2012 shall also be followed. In addition, the following applies.

Subsystems of category 2 shall be designed so that their functional channel (I, L, O) is tested at suitable intervals. The test of the sub-function(s) shall be performed before or at least at the demand of the safety function prior to any hazardous situation, e.g.:

- a) prior to the start of a new cycle;
- b) prior to the start of other movements;
- c) immediately upon demand of the safety function;
- d) periodically during operation if the risk assessment and the kind of operation shows that it is necessary.

The test itself shall not lead to a hazardous situation (e.g. due to an increase in response time). The test equipment may be integral with, or separate from, the safety-related part(s) providing the safety function.

Based on the risk assessment of the machine or part of it, the initiation of this test may be manual. Any test of the sub-function(s) shall either

- allow operation if no faults have been detected, or
- generate an output [output of the test equipment (OTE)] that initiates appropriate control action, if a fault is detected.

For PL_r d the OTE shall initiate a safe state that is maintained until the fault is cleared.

For PL_r up to and including PL_{rc} , whenever practicable the output (OTE) shall initiate a safe state that is maintained until the fault is cleared. When this is not practicable (e.g. welding of the contact in the final switching device) it may be sufficient for the OTE to provide a warning.

The calculation of DC_{avg} shall take into account only the blocks of the functional channel (i.e. I, L and O in [Figure 9](#)) and not the blocks of the testing channel.

For category 2, the following shall be applied:

- demand rate $\leq 0,01$ test rate (see [Table K.1](#), NOTE 1); or testing occurs immediately upon demand of the safety function and the overall time to detect the fault and to bring the machine to a non-hazardous condition (usually to stop the machine) is shorter than the time to reach the hazard (see also ISO 13855:2010).
- $MTTF_D$ of the testing channel (TE and OTE in [Figure 9](#)) is greater than one half of $MTTF_D$ of the functional channel.

The DC of all parts of the functional channel (I, L, O) shall be at least low. The $MTTF_D$ of the functional channel shall be low-to-high, depending on the required performance level (PL_r). Measures against CCF of the functional channel and the testing channel shall be applied (see [6.1.6](#) and [Annex F](#)).

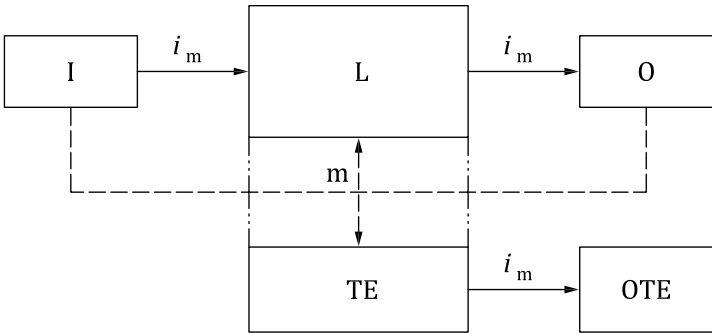
The maximum PL achievable with category 2 is PL d.

NOTE 1 The test of the blocks in the functional channel can be realized by, e.g. monitoring.

NOTE 2 Category 2 system behaviour can be characterized by

- the occurrence of a fault leading to the loss of the sub-function between tests, and
- the loss of sub-function being detected by the tests.

NOTE 3 The principle that supports the validity of a category 2 function is that the adopted technical provisions, and, for example, the choice of test rate and reliability of the test equipment, can decrease the probability of occurrence of a dangerous fault.



Key

- | | | | |
|-------|---------------------------|-----|------------------------------------|
| i_m | interconnecting means | O | output device, e.g. main contactor |
| I | input device, e.g. sensor | TE | test equipment |
| L | logic | OTE | output of TE |
| m | monitoring/testing | | |

The dashed lines represent reasonably practicable fault detection.

Figure 9 — Designated architecture for category 2