



DPC: 20/30360575 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 08 June 2020

Origin: European

Latest date for receipt of comments: 01 August 2020

Project No. 2017/01559

Responsible committee: MCE/3 Safeguarding of machinery

Interested committees:

Title: Draft BS EN ISO 13849-1 Safety of machinery — Safety-related parts of control systems. Part 1: General principles for design.

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 01 August 2020

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/Figure/ Table/Note	Type of comment	Commend (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	

DRAFT INTERNATIONAL STANDARD

ISO/DIS 13849-1

ISO/TC 199

Secretariat: DIN

Voting begins on:
2020-06-08

Voting terminates on:
2020-08-31

Safety of machinery — Safety-related parts of control systems —

Part 1: General principles for design

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

ICS: 13.110

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING



Reference number
ISO/DIS 13849-1:2020(E)

AVA Documents
Document Sharing Hub
© ISO 2020



COPYRIGHT PROTECTED DOCUMENT

© ISO 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	vi
Introduction	vii
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
3.1 Terms and definitions	2
3.2 Symbols and abbreviated terms	10
4 Overview	11
4.1 Requirements for risk assessment and risk reductions	11
4.2 Contribution to the risk reduction by the safety function	13
4.3 Risk reduction using an SRP/CS	13
4.4 Methodology	15
4.5 Required Information	15
4.6 Safety function realization by using subsystems	16
5 Specification of safety functions	16
5.1 General	16
5.2 Safety requirements specification (SRS)	17
5.2.1 General requirements	17
5.2.2 Decomposition of SRP/CS into subsystems	19
5.2.3 Requirements for specific safety functions	20
5.3 Determination of required performance level (PL _r) for each safety function	25
5.4 Review of the safety requirement specification	25
6 Design considerations	25
6.1 Evaluation of the achieved performance level PL	25
6.1.1 General overview of Performance level PL	25
6.1.2 Correlation between PL and SIL	27
6.1.3 Architecture – Categories and their relation to MTTF _D of each channel, DC _{avg} and CCF	27
6.1.4 Mean time to dangerous failure (MTTF _D)	34
6.1.5 Diagnostic coverage (DC)	35
6.1.6 Common cause failures (CCF)	36
6.1.7 Systematic failures	36
6.1.8 Simplified procedure for estimating the PL	36
6.1.9 Alternative procedure to determine the PL and PFH _D without MTTF _D	38
6.1.10 Fault consideration and fault exclusion	39
6.1.11 Well-tried component	41
6.2 Combination of subsystems to achieve an overall PL of the safety function	41
6.2.1 General	41
6.2.2 Known PFH _D values	41
6.2.3 Unknown PFH _D values	42
7 Software safety requirements	42
7.1 General	42
7.2 Safety-related embedded software (SRESW)	43
7.3 Safety-related application software (SRASW)	45
7.4 Limited variability language (LVL)	47
7.4.1 General	47
7.4.2 Full variability language (FVL)	48
7.4.3 Decision for LVL or FVL	48
7.5 Software-based parameterization	50
7.5.1 General	50
7.5.2 Influences on safety-related parameters	50
7.5.3 Requirements for software based manual parameterization	50

7.5.4	Verification of the parameterization tool	52
7.5.5	Performance of software based manual parameterization	52
8	Verification that achieved PL meets PL_r	53
9	Ergonomic aspects of design	53
10	Validation	53
10.1	Validation principles	53
10.1.1	General	53
10.1.2	Validation plan	55
10.1.3	Generic fault lists	56
10.1.4	Specific fault lists	56
10.1.5	Information for validation	56
10.2	Validation by analysis	57
10.2.1	General	57
10.2.2	Analysis techniques	58
10.3	Validation by testing	58
10.3.1	General	58
10.3.2	Measurement accuracy	59
10.3.3	Additional requirements for testing	59
10.3.4	Number of test samples	59
10.3.5	Testing methods	59
10.4	Validation of the Safety Requirements Specification (SRS)	60
10.5	Validation of the safety function	60
10.6	Validation of the safety integrity of the SRP/CS	61
10.6.1	Validation of subsystem(s)	61
10.6.2	Validation of measures against systematic failures	62
10.6.3	Validation of safety-related software	63
10.6.4	Validation of combination of subsystems	63
10.6.5	Checking/verification of safety integrity	64
11	Maintenance	64
12	Technical documentation	64
13	Information for use	65
13.1	General	65
13.2	Information for SRP/CS integrator	65
13.3	Information for user	66
Annex A (informative)	Determination of required performance level (PL_r)	68
Annex B (informative)	Block method and safety-related block diagram	72
Annex C (informative)	Calculating or evaluating MTTF_D values for single components	74
Annex D (informative)	Simplified method for estimating MTTFD for each channel	81
Annex E (informative)	Estimates for diagnostic coverage (DC) for functions and modules	83
Annex F (informative)	Measures against common cause failures (CCF)	88
Annex G (informative)	Systematic failure	92
Annex H (informative)	Example of combination of several subsystems	95
Annex I (informative)	Examples	97
Annex J (informative)	Software	105
Annex K (informative)	Numerical representation of Figure 12	108
Annex L (informative)	EMC immunity requirements	113
Annex M (informative)	Additional Information for Safety Requirements Specification	115
Annex N (informative)	Avoiding of systematic failure in software-design	117

Anhang ZA (informative) Relationship between this European Standard and the essential requirements of EU Directive 2006/42/EC aimed to be covered.....	124
Bibliography	125

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*.

The first edition of ISO 13849-1 was published in 1999 based on EN 954-1:1996.

The second edition of ISO 13849-1 was revised in 2006.

The third edition was amended and published in 2015.

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

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

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

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

- a) Type-A standards (basis standards) give basic concepts, principles for design and general aspects that can be applied to machinery.
- b) Type-B standards (generic safety standards) deal with one or more safety aspect(s), or one or more type(s) of safeguards that can be used across a wide range of machinery:
 - type-B1 standards on particular safety aspects (e.g. safety distances, surface temperature, noise);
 - type-B2 standards on safeguards (e.g. two-hands 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 part of ISO 13849 is a type-B-1 standard as stated in ISO 12100.

This document is of relevance, in particular, for the following stakeholder groups representing the market players with regard to machinery safety:

- machine manufacturers (small, medium and large enterprises);
- health and safety bodies (regulators, accident prevention organisations, market surveillance etc.).

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

- machine users/employers (small, medium and large enterprises);
- machine users/employees (e.g. trade unions, organizations for people with special needs);
- service providers, e.g. for maintenance (small, medium and large enterprises);
- consumers (in case of machinery intended for use by consumers).

The above-mentioned stakeholder groups have been given the possibility to participate at the drafting process of this document.

In addition, this document is intended for standardization bodies elaborating type-C standards.

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

When provisions of a type-C standard are different from those which are stated in type-A or type-B standards, the provisions of the type-C standard take precedence over the provisions of the other standards for machines that have been designed and built according to the provisions of the type-C standard.

NOTE 1 The examples and basis for most content is based on stationary machines in factory applications. However, other machines are not excluded. This document was written with the intent of being used across many machinery industries and as a basis for type-C standards developers.

This part of ISO 13849 is intended to give guidance to those involved in the design and assessment of control systems, and to Technical Committees preparing type-B2 or type-C standards.

Risk reduction according to ISO 12100:2010, Clause 6, is accomplished by applying, in the following sequence, inherently safe design measures, safeguarding and/or complementary risk reduction measures and information for use. A designer may reduce risks by risk reduction measures that can have safety functions. Parts of machinery control systems that are assigned to provide safety functions are called safety-related parts of control systems (SRP/CS). These can consist of hardware and/

or software, and can either be separate from the machine control system or an integral part of it. In addition to implementing safety functions, SRP/CS can also implement operational functions.

ISO 12100 is used for risk assessment of the machine. ISO 13849-1, Annex A, can be used for the determination of the required performance level of a safety function performed by the SRP/CS, where PL_r is not specified in the applicable type-C standard.

ISO 13849-1 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 has initiated a risk reduction measure (e.g. interlocking guard) that relies on a safety-related control system. In those cases, the safety-related control system has to perform a safety function. ISO 13849-1 should be used to design and evaluate the safety-related parts of the control system. Only the part of the control system that is safety-related falls under the scope of ISO 13849-1.

[Figure 1](#) illustrates the relationship between ISO 12100 and ISO 13849-1.

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

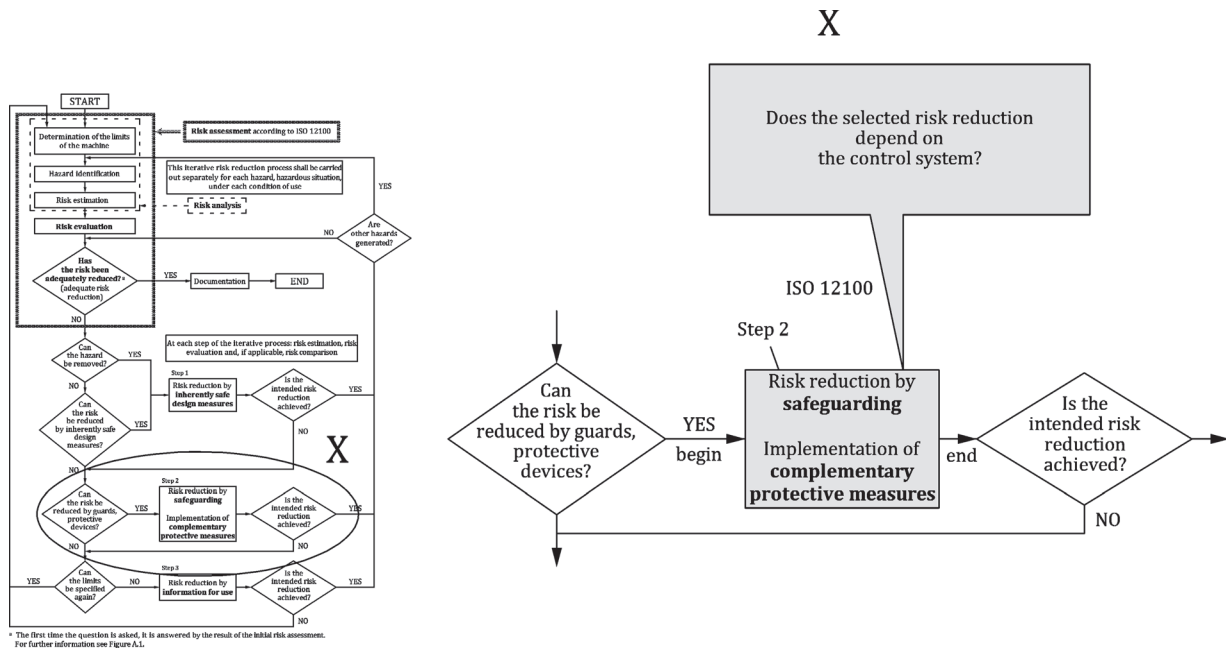


Figure 1 — Integration of ISO 13849-1 within the risk reduction process of ISO 12100

NOTE 3 [Figure 1](#) shows where the SRP/CS contributes to the risk reduction process of ISO 12100: 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 (PLr) for a particular safety function will be determined by risk estimation.

The probability of dangerous failure of the safety function depends on several factors, including hardware and software structure, the extent of fault detection mechanisms [diagnostic coverage (DC)], reliability of components [mean time to dangerous failure (MTTF_D)], common cause failure (CCF), design process, operating stress, environmental conditions and operation procedures.

Functional safety includes a categorization of architecture according to specific design and specified behaviours under fault conditions. This architecture is allocated one of five 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 probability of dangerous failure per hour (PFH_D).

Risk estimation will show a variance because of the subjective nature of the evaluation criteria. Type-C standards can have more specific risk estimation methods for specific machine applications, which can be less subjective in nature. Therefore, using the methodology in this document should be considered as valuable guidance for the design of the safety-related parts of the control system rather than a strict requirement. The performance levels and categories can be applied to safety-related parts of control systems, such as

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

The performance levels can be calculated, and categories determined for

- SRP/CS performing safety functions for machinery,
- subsystems of SRP/CS using safety parts (components) such as
- protective devices (e.g. two-hand control devices, interlocking devices);
- power control elements (e.g. relays, valves);
- Sensors and HMI elements (position sensors, enable switches).

Machinery considered by this standard can range from simple (e.g., small kitchen machines, or automatic doors and gates) to complex (e.g., packaging machines, printing machines, presses).

IEC 62061 and this part of ISO 13849 both specify a methodology and provide related guidance for the design and implementation of safety-related control systems of machinery.

NOTE ISO/TR 23849 gives guidance on the relation between both standards, how they complement each other.

The requirements of Clause 10 of ISO 13849-1 supersede the requirements of ISO 13849-2:2012 with the exception of the informative annexes. An SRP/CS that meets the requirements of [Clause 10](#) is considered to meet the requirements of ISO 13849-2:2012.

Safety of machinery — Safety-related parts of control systems —

Part 1: General principles for design

1 Scope

This part of ISO 13849 specifies a methodology and provides related guidance for the design and integration of safety-related parts of control systems (SRP/CS), including the design of software. This document specifies the characteristics needed to determine the performance level required of safety functions. This document applies to SRP/CS for high demand and continuous mode including their subsystems, regardless of the type of technology and energy (e.g. electrical, hydraulic, pneumatic, mechanical), for many kinds of machinery. The standard does not apply to low demand mode.

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

This document does not give specific requirements for the design of products that are parts of SRP/CS.

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

NOTE 1 This document specifies a methodology for SRP/CS design without considering if certain machinery (e.g. mobile machinery) requires specific requirements. These specific requirements can be considered in a Type-C standard.

NOTE 2 See IEC 61508 for low demand mode.

NOTE 3 See also ISO/TR 22100-4 for IT-security aspects and IEC/TR 63074 for security aspects.

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 13849-2:2013, *Safety of machinery — Safety-related parts of control systems — Part 2: Validation*

IEC 60204-1:2016, *Safety of machinery — Electrical equipment of machines — Part 1: General requirements*

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*

ISO 62061:2015, *Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems*

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <https://www.iso.org/obp>

3.1 Terms and definitions

3.1.1

safety-related part of a control system

SRP/CS

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

Note 1 to entry: The safety-related parts of a control system starts 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

safety requirement specification

SRS

specification containing the requirements for the safety functions that have to be performed by the safety related control system in terms of characteristics of the safety functions (functional requirements) and required performance levels

[SOURCE: IEC 61508-4:2010, 3.5.11 and 3.5.12, modified, NOTE added]

3.1.3

category

classification of the subsystem in respect of the resistance to faults 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

3.1.4

fault

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

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

Note 2 to entry: In this part of ISO 13849-1, “fault” means random fault or fault caused by a systematic failure.

[SOURCE: IEC 60050-192:2015; modified: NOTE 2 to entry amended]

3.1.5

fault exclusion

exclusion of certain faults within an SRP/CS, if this can be justified due to their improbability and their negligible contribution to the reliability of the SRP/CS

3.1.6

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.

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 part of ISO 13849.

[SOURCE: IEC 60050-192:2015; modified: NOTE 4 to entry amended]

3.1.7**dangerous failure**

failure which has the potential to put the SRP/CS in a hazardous or fail-to-function state

Note 1 to entry: Whether or not the potential is realized can depend on the channel architecture of the system; in redundant systems a dangerous hardware failure is less likely to lead to the overall dangerous or fail-to-function state.

[SOURCE: IEC 61508-4:2010, 3.6.7]

3.1.8**common cause failure****CCF**

failure, that is the result of one or more events, causing concurrent failures of two or more separate channels in a multiple channel subsystem, leading to failure of a safety function

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

[SOURCE: IEC 61508-4:2010]

3.1.9**systematic failure**

failure 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,
- the design, manufacture, installation, operation of the hardware, and
- the design, implementation, etc., of the software.

[SOURCE: IEC 60050-192:2015]

3.1.10**muting**

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

3.1.11**manual reset**

safety function within the SRP/CS used to restore manually one or more safety functions before re-starting a machine

3.1.12**harm**

physical injury or damage to health

[SOURCE: ISO 12100:2010, 3.5]

3.1.13**hazard**

potential source of harm

Note 1 to entry: A 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 deleted]

3.1.14

hazardous situation

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

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

[SOURCE: ISO 12100:2010, 3.10]

3.1.15

risk

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

[SOURCE: ISO 12100:2010, 3.12]

3.1.16

residual risk

risk remaining after risk reduction measures (protective measures) have been taken

Note 1 to entry: See [Figure 2](#).

[SOURCE: ISO 12100:2010, 3.13, Note 1 modified]

3.1.17

risk assessment

overall process comprising risk analysis and risk evaluation

[SOURCE: ISO 12100:2010, 3.17]

3.1.18

risk analysis

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

[SOURCE: ISO 12100:2010, 3.15]

3.1.19

risk evaluation

judgement, on the basis of risk analysis, of whether risk reduction objectives have been achieved

[SOURCE: ISO 12100:2010, 3.16]

3.1.20

intended use of a machine

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

[SOURCE: ISO 12100:2010, 3.23]

3.1.21

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]

3.1.22**safety function**

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

Note 1 to entry: A safety function is a function to be 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]

3.1.23**monitoring**

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

Note 1 to entry: Monitoring is realised by following methods: plausibility check (direct or indirect monitoring), cyclic test stimulus or cross monitoring

3.1.24**cross monitoring**

diagnostic measure which checks plausibility of redundant signals in both channels of a redundant logic unit

3.1.25**programmable electronic system****PE system**

system for control, protection or monitoring 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]

3.1.26**performance level****PL**

discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions

Note 1 to entry: See [6.1](#).

3.1.27**required performance level****PL_r**

performance level (PL) applied in order to achieve the required risk reduction for each safety function

Note 1 to entry: See [Figure 2](#) and [Figure A.1](#).

3.1.28**mean time to dangerous failure****MTTF_D**

expected value of 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 62061:2005, 3.2.34, NOTE 1 to entry modified]

3.1.29**mean time between failure****MTBF**

expected value of the operating time between consecutive failures

3.1.30

ratio of dangerous failures

RDF

fraction of the overall failure rate of an element that can result in a dangerous failure

3.1.31

diagnostic coverage

DC

measure of the effectiveness of diagnostics, which is determined as the ratio between the failure rate of detected dangerous failures 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 could exist for sensors and/or logic system and/or power control elements.

[SOURCE: IEC 61508-4:2010, 3.8.6]

3.1.32

risk reduction measure

protective measure

action or means to eliminate hazards or reduce risks

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

[SOURCE: ISO Guide 51:2014, 3.13]

3.1.33

mission time

T_M

period of time covering the intended use of an SRP/CS

Note 1 to entry: to entry: Typically, by reaching the mission time the SRP/CS is replaced.

3.1.34

test rate

r_t

frequency of automatic tests to detect faults in an SRP/CS, reciprocal value of diagnostic test interval

3.1.35

demand rate

r_d

frequency of demands for a safety function to be executed by the SRP/CS

3.1.36

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).

3.1.37

safety integrity level

SIL

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

[SOURCE: IEC 61508-4:2010, 3.5.8]

3.1.38**limited variability language****LVL**

type of language that provides the capability of combining predefined, application-specific library functions and basic logic to implement the safety requirements specifications

Note 1 to entry: Typical examples of LVL (ladder logic, function block diagram) are given in IEC 61131-3.

[SOURCE: IEC 61511-1:2017, 3.2.75.2]

3.1.39**full variability language****FVL**

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

Note 1 to entry: In the field of machinery, FVL as C, C++ assembler is typically found in embedded software and rarely in application software.

[SOURCE: IEC 61511-1:2017, 3.2.75. 3, modified: NOTE 1 to entry deleted; NOTE 2 to entry amended]

3.1.40**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 SRP/CS requirements

3.1.41**Safety related embedded software****SRESW**

firmware

system software

software that is part of the system supplied by the manufacturer and is not accessible for modification by the user of the machinery

Note 1 to entry: Embedded software is usually written in FVL.

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

3.1.42**high demand or continuous mode**

mode of operation in which the frequency of demands on an SRP/CS to perform its safety function 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]

3.1.43**low demand mode**

mode of operation in which the frequency of demands on the SRP/CS to perform its safety function is not greater than once per year

Note 1 to entry: Low demand mode is not addressed in this document, see [Clause 1](#).

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

3.1.44

subsystem

entity which results from a first-level decomposition of an SRP/CS and whose dangerous failure results in a dangerous failure of a safety function

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 for de-energise a motor in case of detection of a person in a danger zone and also in case of opening a safe guard.

3.1.45

subsystem element

part of a subsystem comprising a single component or any group of components not solely being able to carry out a safety function

Note 1 to entry: A subsystem element can comprise hardware and software, e.g. sensor, contactor.

3.1.46

well-tried safety principle

principles that have proved effective in the design or integration of safety-related control systems in the past, to avoid or control critical faults or failures which can influence the performance of a safety function

Note 1 to entry: Newly developed safety principles can only be considered as equivalent to “well-tried” if they are verified using principles 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 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: [Table A.2](#), Table B.2, [Table C.2](#) and Table D.2 in the informative annexes of ISO 13849-2 address well-tried safety principles for different technologies.

3.1.47

well-tried component

component proven to be successfully used in previous safety-related applications

Note 1 to entry: to entry: See [6.1.11](#) for requirements and ISO 13849-2 for a list of recognized well-tried components.

3.1.48

operating mode

mode of operation in a machine (i.e. 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 and/or protective measures 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

dynamic test

diagnostic measure which regularly executes a change of a signal for test purposes, which is monitored

Note 1 to entry: The test failed if monitoring 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. For short circuit detection a time delay is necessary between the test pulses e.g. with different frequency.

3.1.50**plausibility check**

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

3.1.51**safety sub-function**

part of a safety function whose failure can result in a failure of the safety function

Note 1 to entry: A safety sub-function is a function to be implemented by a subsystem of the SRP/CS.

EXAMPLE Safety sub-functions according to EN 61800-5-2 are e.g. safe torque off (STO), safe stop 1 (SS1).

3.1.52**channel**

element or group of elements that independently implement a safety function or a part of it

[SOURCE: IEC 61508-4:2010, 3.3.6]

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, modified, “by the SRP/CS” added]

3.1.54**validation**

confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled by the SRP/CS

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: ISO 9000:2015, 3.8.13, modified, “by the SRP/CS” added]

3.1.55**permanent fault**

fault of an item that persist until an action of corrective maintenance is performed

[SOURCE: IEC 60050-192:2015]

3.1.56**skilled person**

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

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

[SOURCE: ISO 14990-1:2016, 3.5.4, modified “electricity” replaced by “the relevant equipment”]

3.2 Symbols and abbreviated terms

[Table 1](#) gives an overview on used abbreviations and terms.

Table 1 — Symbols and abbreviated terms

Symbol or abbreviation	Description	Definition or occurrence
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 4
B_{10D}	Number of cycles until 10 % of the components fail dangerously (for components with mechanical wear)	Annex C
Cat.	Category	3.1.3
CC	Current converter	Annex I
CCF	Common cause failure	3.1.8
DC	Diagnostic coverage	3.1.31
DC_{avg}	Average diagnostic coverage	E.2
EMI	Electromagnetic interference	6.2.2
ETA	Event tree analysis	10.3.2
F, F1, F2	Frequency and/or time of exposure to the hazard	A.2.2
FB	Function block	Annex J
FVL	Full variability language	3.1.40
FMEA	Failure modes and effects analysis	6.1.5
FMECA	Failure modes, effects and critically analysis	10.3.2
FTA	Fault tree analysis	10.3.2
$F(t)$	cumulated distribution function	Annex 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 and E.2
i_m	Interconnecting means	Figure 7, 8, 9, 10
K1A, K1B	Contactors	Annex I
L, L1, L2	Logic	6.1
LVL	Limited variability language	3.1.38
λD	Dangerous failures of a component	Annex C
M	Motor	Annex I
MTTF	Mean time to failure	Annex C
$MTTF_D$	Mean time to dangerous failure	3.1.28
$n, N, \tilde{N}$	Number of items	6.2, D.1
N_{low}	Number of SRP/CS with PL_{low} in a combination of SRP/CS	6.2
n_{op}	Mean number of annual operations	Annex C
O, O1, O2, OTE	Output device, e.g. power control elements	6.1
P, P1, P2	Possibility of avoiding the hazard	A.2.3
PES	Programmable electronic system	3.1.26
PFH_D	average probability of dangerous failure per hour	Table 2 and Table K.1
PL	Performance level	3.1.27
PLC	Programmable logic controller	Annex I

Table 1 (continued)

Symbol or abbreviation	Description	Definition or occurrence
PL_{low}	Lowest performance level of an SRP/CS in a combination of SRP/CS	6.2
PL_r	Required performance level	3.1.27
r_d	Demand rate	3.1.35
r_t	Test rate	3.1.34
RDF	Ratio of Dangerous failures	Annex C.4.2
RS	Rotation sensor	Annex I
S, S1, S2	Severity of injury	A.2.1
SB	Subsystem	Figure 13, H.1, H.2
SW1A, SW1B, SW2	Position switches	Annex I
SIL	Safety integrity level	3.1.38, Clause 5
SRASW	Safety-related application software	3.1.40
SRESW	Safety-related embedded software	3.1.41
SRP	Safety-related part	General
SRP/CS	Safety-related part of a control system	3.1.1
SRS	Safety requirement specification	3.1.2
TE	Test equipment	6.1
T_M	Mission time	3.1.33
T_{10D}	Mean time until 10 % of the components fail dangerously	Annex C

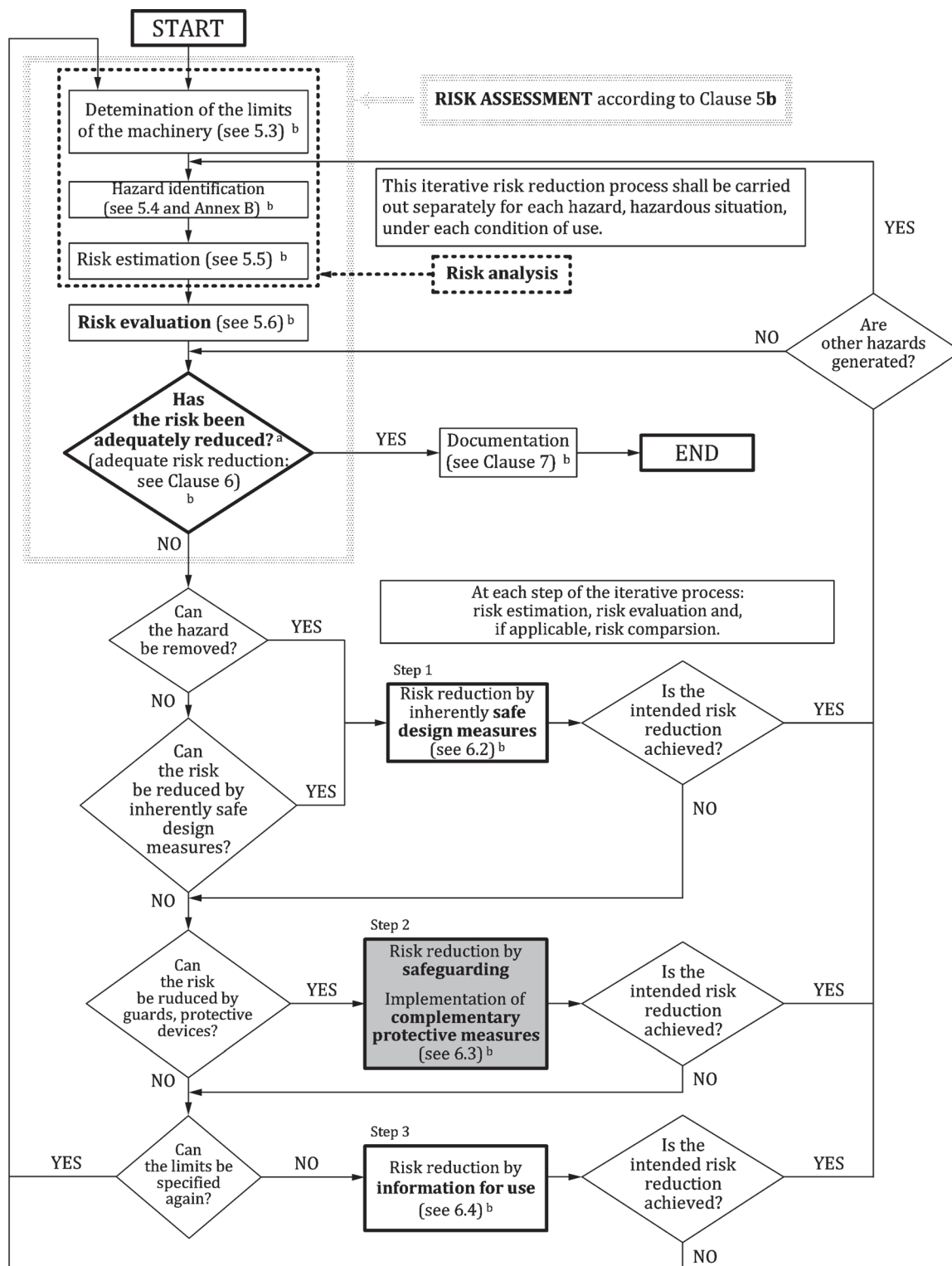
4 Overview

4.1 Requirements for risk assessment and risk reductions

Risk assessment process is defined by ISO 12100 as shown in [Figure 1](#). ISO 13849-1 is included in the risk assessment and risk reduction process when a safety function and its corresponding control system are used to perform the risk reduction.

The safety requirements specification 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 3](#)).

NOTE This document does not apply to non-safety related parts of control systems of a machine (see [Figure 5](#)).



^a The first time the question is asked, it is answered by the result of the initial risk assessment.

^b refers to ISO 12100:2010

■ Risk reduction by safeguarding may be realized by SRP/CS which execute safety functions.
In this case ISO 13849 applies, see Figure 3.

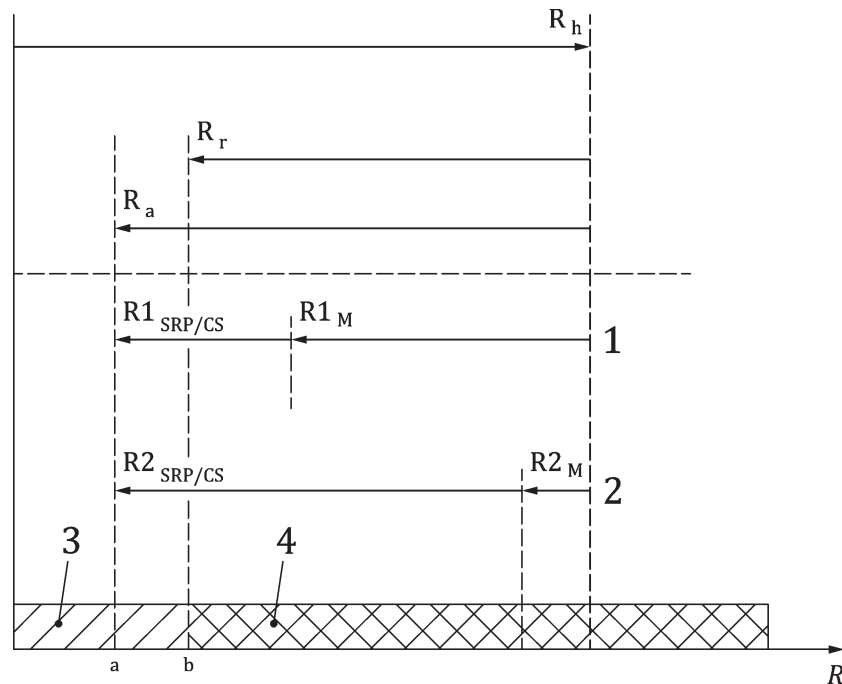
Figure 2 — Schematic representation of risk reduction process including iterative three-step method according to ISO 12100:2010

NOTE In special cases ISO 13849-1 applies also to step 3, for examples see [Annex M](#) for indications and alarms.

4.2 Contribution to the risk reduction by the safety function

From the risk assessment, the designer shall decide the contribution to the reduction of risk 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. It does not cover the overall risk of machinery under control.

NOTE Examples of such functions are the stopping function initiated by using an electro-sensitive protective device on a press or the door-locking function of a washing machine.



Key

R_h	for a specific hazardous situation, the risk before protective measures are applied
R_r	risk reduction required from protective measures
R_a	actual risk reduction achieved with protective measures
1	Solution 1 – important part of risk reduction due to protective measures other than SRP/CS (e.g. mechanical measures), small part of risk reduction due to SRP/CS
2	solution 2 – important part of risk reduction due to the SRP/CS (e.g. light curtain), small part of risk reduction due to protective measures other than SRP/CS (e.g. mechanical measures)
3	adequately reduced risk
4	inadequately reduced risk
R	risk
a	residual risk obtained by solutions 1 and 2
b	adequately reduced risk
$R1_{SRP/CS}$, $R2_{SRP/CS}$	risk reduction from the safety function carried out by the SRP/CS
$R1_M$, $R2_M$	risk reduction from protective measures other than SRP/CS (e.g. mechanical measures)

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

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

4.3 Risk reduction using an SRP/CS

Figure 4 shows the design process of safety functions implemented by SRP/CSs, and the determination of whether the safety functions achieve the intended risk reduction.

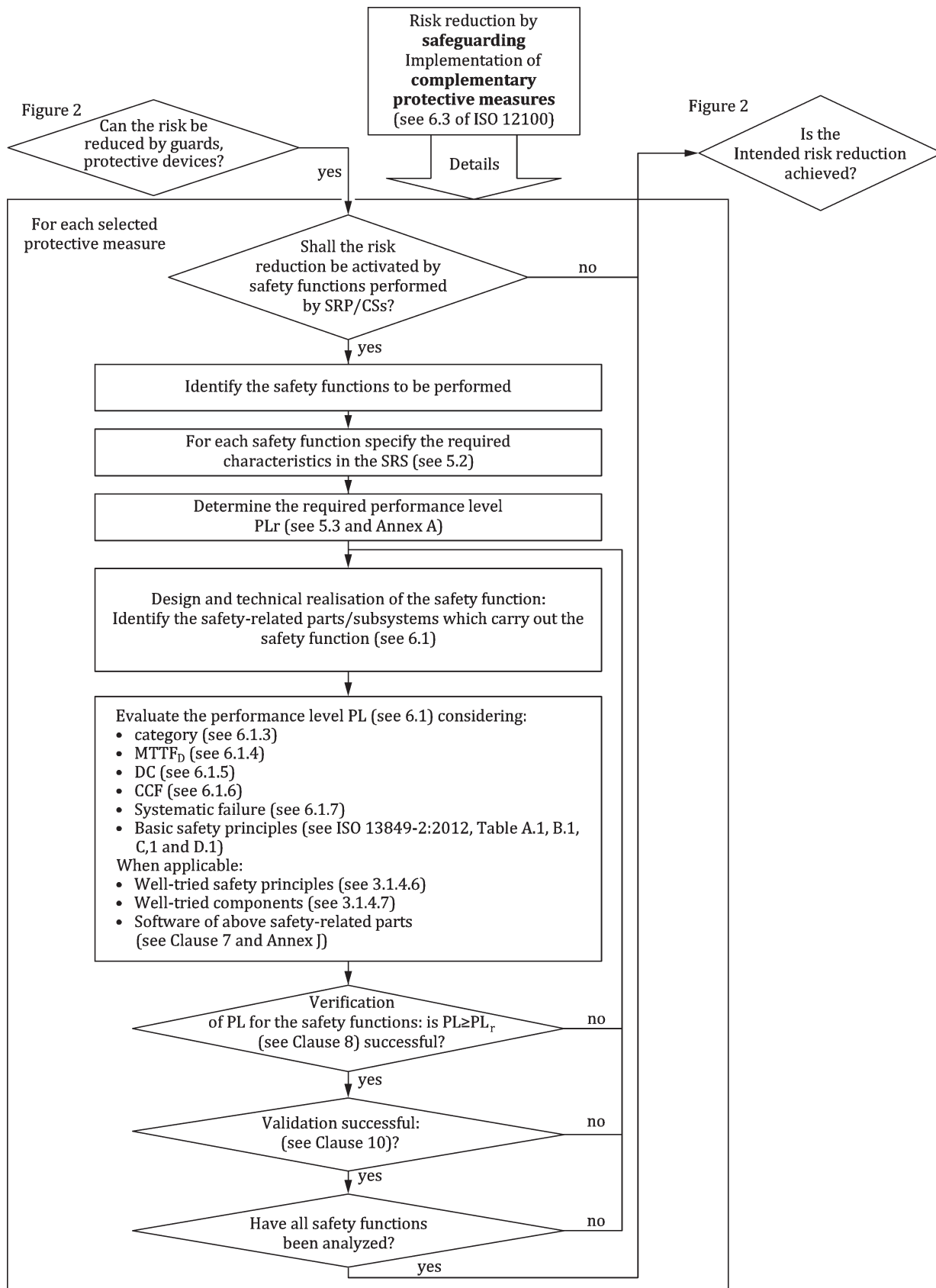


Figure 4 — Iterative process for design of safety-related parts of control systems (SRP/CS)

4.4 Methodology

This document uses the following methodology:

- 1) specifying the required characteristics for each safety function ([5.2](#));
- 2) determining a required performance level (PL_r) for each safety function (see [5.3](#));
- 3) design and technical realization of the safety functions including identification of the SRP/CSs and their subsystems which carry out each safety function;
 - a) Design considerations ([Clause 6](#)),
 - b) Software safety requirements ([Clause 7](#));
- 4) Verification that the achieved PL meets PL_r ([Clause 8](#));
- 5) Ergonomic aspects of the design ([Clause 9](#));
- 6) Validation ([Clause 10](#) or ISO 13849-2);
- 7) Maintenance ([Clause 11](#));
- 8) Technical documentation ([Clause 12](#));
- 9) Information for use ([Clause 13](#)).

The required performance level refers to the risk reduction to be provided by the safety function. The greater the risk reduction, the higher the required safety performance shall be.

The performance levels are defined in terms of average probability of dangerous failure of the safety function per hour. There are five performance levels, from providing the least risk reduction PL a to the greatest risk reduction PL e. The defined ranges of probability of a dangerous failure per hour are in [Table 2](#).

Table 2 — Performance levels (PL)

PL	Average probability of dangerous failure per hour (PFH _D) 1/h
a	$10^{-5} \leq \text{PFH}_D < 10^{-4}$
b	$3 \times 10^{-6} \leq \text{PFH}_D < 10^{-5}$
c	$10^{-6} \leq \text{PFH}_D < 3 \times 10^{-6}$
d	$10^{-7} \leq \text{PFH}_D < 10^{-6}$
e	$\text{PFH}_D < 10^{-7}$

Subsystems shall be evaluated using the same process as is used for SRP/CS systems, according to [Clause 5](#) through [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;
- 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 (see [5.2](#));

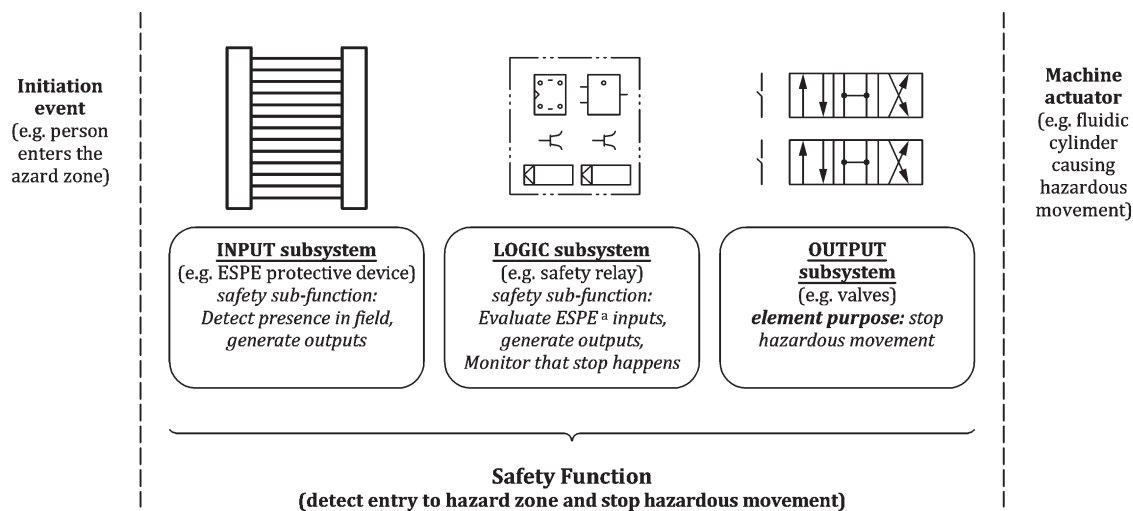
- determination of the required performance level (PL_r) for each safety function (see 5.3).

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

4.6 Safety function realization by using subsystems

The realisation of a safety function to achieve the required PL may be done by the design of SRP/CS:

- using previously validated subsystems according to this document or IEC 62061, IEC 61508 or other relevant safety related product standards (e.g. IEC 61496-1 and IEC 61800-5-2), or
- designing new subsystems according to this document, or
- a combination of both alternatives above (see example in Figure 5).



Key

- ^a Electrosensitive protective equipment (ESPE)

Figure 5 — Example of combination of subsystems

5 Specification of safety functions

5.1 General

The objective of this sub clause 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 and afterwards as a part of the design specification for the SRP/CS under ISO 13849-1.

This subclause addresses the following steps:

- 1) General description of the safety function (linking hazards to safety functions)
- 2) Detailed description of the safety requirements (see 5.2);
- 3) NOTE For specific safety functions additional requirements see 5.2.3.

- 4) Determination of the PL_r for each safety function (how reliable the safety function needs to be – see 5.3);
- 5) Review of the safety requirement specification (see 5.4).

A safety function shall have a general description to define how the SRP/CS contributes to reduce risk. 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.

5.2 Safety requirements specification (SRS)

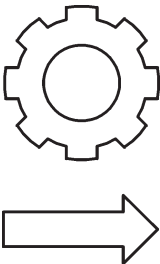
5.2.1 General requirements

5.2.1.1 General

The safety requirements specification shall document details of each safety function to be performed.

NOTE 1 The safety requirement specification is very important to avoid mistakes at the transition from the risk assessment and risk reduction process according to ISO 12100 to the SRP/CS design and evaluation process according to ISO 13849, 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 to the SRP/CS design and evaluation process according to ISO 13849

Necessary information to produce the SRS (see 5.2.1.2)		Specification of all safety functions in the SRS (see 5.2.1.3)
— Results of risk assessment, including hazardous parts — 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 — Mode of operation (all) — Triggering event: opening of a movable guard — Safety-related reaction: safe torque off (STO) of all movements — PL_r e.g. d — response time: e.g. 200 ms — ... 2) Safely Limited Speed (SLS) — Mode of operation (manual) — Triggering event: Speed is higher than the specified limit — Safety-related reaction: safe torque off (STO) of all movements — PL_r e.g. c — response time: e.g. 150 ms — ...

5.2.1.2 Necessary information to produce the SRS

The following information should be used by the designer of the safety-related control system to produce the safety requirements specifications:

- a) Results of the risk assessment for each specific hazard where the associated risk reduction measure(s) rely 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) modes of operation (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 (see also ISO 13855, 5.1);

NOTE 1 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 2 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 (see ISO 12100, 3.39 and IEC 60204-1, 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 prevent incorrect operation or defeating;
- f) limits of use in relation to environmental condition

5.2.1.3 Specification of all safety functions in the SRS

The designer shall include the following information necessary to achieve the measures of safety required of the control system for the specific application:

Brief description / title of the safety function to have a clear reference;

- a) the event that triggers the safety function;
- b) the required performance level PL_r for each safety function (see 5.3);

NOTE 1 If necessary define the required category (see 6.1.3).

- c) the safety-related reaction of the machine caused by the safety function output(s);

EXAMPLE 1 Safe stop of a hazardous movement

- d) 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;
- e) the mode(s) of operation during which the safety function is to be active;
- f) all interfaces between the safety functions, and between safety functions and any other non-safety functions (either within or outside the machine);

EXAMPLE 2 A safety function may be muted to allow the transport of material to or from a dangerous area.

- g) if needed, alternative reactions to bring the machine to a safe state in case of a fault in a functional channel including how the safe state is maintained until the fault is repaired;

EXAMPLE 3 The hydraulic pump may be switched off to stop the movement of a cylinder in case of a detected fault in a valve.

- h) the behaviour of the machine on the loss of power (see also [5.2.3.7](#));

NOTE 2 In some cases it can be necessary to consider the behaviour of the machine on loss of power for example when it is necessary to hold a vertical axis to prevent a fall under gravity. This can require two separate safety functions: with power available and without power available. An emergency stop shall be available at all times and override all other functions.

- i) the demand rate or frequency of operation;
- j) the priority of the safety functions that can be simultaneously active and that can cause conflicting action.

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

EXAMPLE 5 The safety function "safe limited speed" (see IEC 61800-5-2, 4.2.3.4) can be a precondition of a safety function "hold to run".

The above is a non-exhaustive list of details for safety functions which can be provided by the SRP/CS.

Where type-C standards or other relevant standards specify safety requirements for the design of an SRP/CS or subsystem (e.g. ISO 23125, ISO 13851) these should be considered.

For operational functions which can have both operational and safety functions the designer or the developers of the Type-C-Standard should indicate the safety function carried out and the PL_r assigned to the respective safety function.

See also [Annex M](#).

5.2.2 Decomposition of SRP/CS into subsystems

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

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

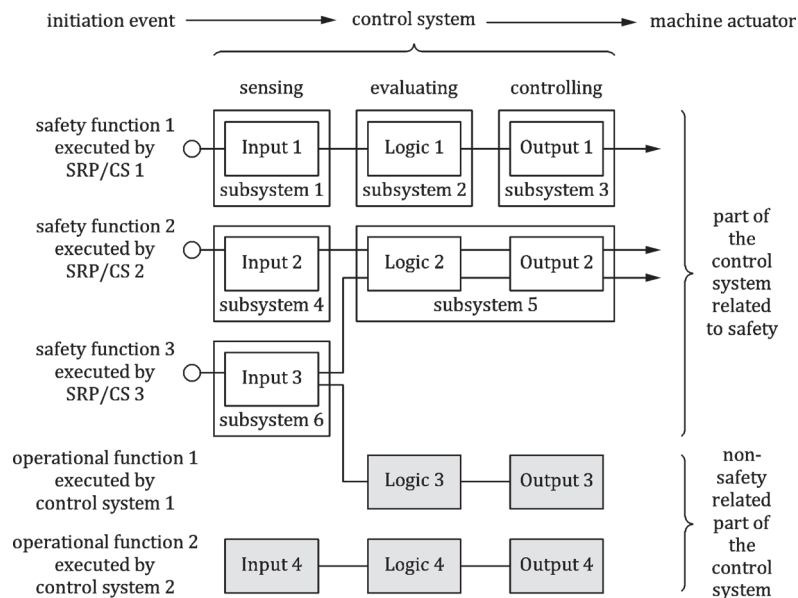
An SRP/CS can comprise:

- one or several previously validated subsystem(s);
- one or several subsystem(s) based on subsystem element(s).

By definition, a dangerous failure ([3.1.7](#)) of any subsystem ([3.1.44](#)) can result in the loss of the whole safety function.

NOTE 1 An SRP/CS can be defined by one single subsystem having a sensor, logic and power control elements. 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 laser beam).

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 is ending with an output causing a reaction of a 'machine actuator' (e.g. motor, cylinder).



Key

- Safety function 1 is decomposed into sub-function 1, sub-function 2 and sub-function 3. Sub-function 1 is executed by subsystem 1, etc.
- Safety function 2 is decomposed into sub-function 4 and sub-function 5. Sub-function 4 is executed by subsystem 4, etc.
- Safety function 3 is decomposed into sub-function 6 and sub-function 5. Sub-function 6 is executed by subsystem 6, etc.

Figure 6 — An example of decomposition of a safety function and its allocation to subsystems

Figure 6 shows a diagrammatic presentation of subsystems combined as SRP/CS(s) for:

- 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) (subsystems 3 and 5), and
- 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 realized by a single subsystem or more than three subsystems.

NOTE 2 It is also possible that one subsystem or SRP/CS implements safety functions and standard control functions. The designer can use any of the technologies available, singly or in combination. SRP/CS can also provide an operational function (e.g. an AOPD as a means of cycle initiation).

NOTE 3 The designer of a previously validated subsystem can be a machine manufacturer or a component manufacturer.

NOTE 4 When using a previously validated subsystem the manufacturer of this subsystem will provide the relevant information, see 13.2.

5.2.3 Requirements for specific safety functions

5.2.3.1 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 starts and non-safety-related stops.

When a group of machines is working together in a coordinated manner, provision shall be made for signalling the supervisory control and/or the other machines that such a stop condition exists.

As a result of the risk assessment safe stopping functions can be realised according to the stop categories in IEC 60204-1, 9.2.2, and/ or safe-torque off (STO), safe stop 1 (SS1), safe stop 2 (SS2), safe operating stop (SOS) (IEC 61800-5-2, 4.2.4).

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

5.2.3.2 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 which is separate from start command within the SRP/CS,
- only be achieved if all affected safety functions and safeguards are operative,
- not initiate a hazardous situation by itself,
- be by intended action,
- enable the control system to accept a separate start command,
- be accepted by signal change.

The parts providing the manual reset function shall be selected so that they do not diminish the safety required of the relevant safety function.

When the function “manual reset” is required to be a safety function (e.g., prevention of unexpected start), the required performance level has to be determined

NOTE 1 It is not always necessary that the manual reset function has the same PL_r as the associated safety function.

The reset actuator shall be located outside the hazard zone and in a position from which there is good 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 complete, a special reset procedure is required.

NOTE 2 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 needs to be realized within a limited time before the control system accepts a separate start command.

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

5.2.3.3 Restart function

A restart shall take place automatically only if a hazardous situation cannot exist. In particular, for interlocking guards with a start function, ISO 12100:2010, 6.3.3.2.5 applies.

NOTE A sensor feedback signal to the control system can initiate an automatic restart.

EXAMPLE In automatic machine operations, sensor feedback signals to the control system are often used to control the process flow. If a work piece has come out of position, the process flow is stopped. If the monitoring of the interlocked safeguard does not have a higher priority to the automatic process control, there could be a danger of unexpected restarting of the machine while the operator readjusts the workpiece. Therefore, the automatic restart ought not to 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) provided by the control system is dependent on the result of the risk assessment.

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

5.2.3.4 Local control function

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

- the means for selecting local control shall be situated outside the danger zone;
- it shall only be possible to initiate command by a local control in a zone defined by the risk assessment in order to avoid hazardous situations;
- switching between local and another control shall not create a hazardous situation;
- the control system shall be designed in such a way that the initiation of commands from different control stations do not lead to a hazardous situation. It can be necessary to preclude use of other controls when the local control is operated.

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

5.2.3.5 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 (SIL or PL, see IEC 62061 or ISO 13849-1) 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 of the SRP/CS shall be reinstated.

The performance level of safety-related parts providing the muting function shall be selected so that the inclusion of the muting function does not diminish the safety required by the relevant safety function.

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

5.2.3.6 Safety-related parameters

When safety-related parameters, e.g. position, speed, temperature, time, torque or pressure, deviate from preset limits the safety-related control system shall initiate appropriate measures (e.g. actuation of stopping, warning signal, alarm).

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 system within the safety-related control system should be provided, e.g. check of limits, format and/or logic input values. For additional requirements see [7.4](#).

Product and C-type standards can require a data checking system for some or all manual parameters. See relevant standards.

See also [Table M.2](#) in [Annex M](#).

5.2.3.7 Fluctuations, loss and restoration of power sources

When fluctuations in energy levels outside the design 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](#) in [Annex M](#).

5.2.3.8 Requirements for operating mode selection

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 protection coverage during the transition.

NOTE Other safety functions and/or risk reduction measures not necessary for the selected operating mode can be deactivated according to the risk assessment for the selected operating mode.

The safety function(s) shall fulfil the required PL according to the risk assessment for operating mode selection.

EXAMPLE For working with open safeguards in setting mode the safety function of interlocking is deactivated and at the same time the safety functions of enabling device function and safely limited speed (SLS) are activated. A risk can arise if not all relevant safety functions are activated.

5.2.3.9 Maintenance considerations for Safety Functions

The design of the machine shall take into account maintenance tasks on the machine and provide safety functions for these tasks to be completed with acceptable risk.

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

- setting;
- teaching/programming;
- process/tool changeover;
- cleaning and housekeeping;
- planned or unplanned preventive or corrective maintenance;
- trouble-shooting/fault finding;
- fault diagnosis.

Some maintenance task will require a full isolation of the machine from all power sources and therefore will not rely on the SRP/CS. For other maintenance task (e.g. teaching or trouble shooting) machine movements might need to be made possible while maintenance personnel are inside the hazard zone. In particular, the design of the SRP/CS shall take into account maintenance tasks where certain safety functions may require manual suspension or override. Where necessary, the design of the SRP/CS

shall allow manual suspension or override tasks to be performed with acceptable risk by providing alternative safety function (e.g. enabling device functions and limiting speed function).

Additional safety functions related to maintenance can be for example:

- Hold-to-run function;
- Enabling Device function;
- Monitoring or limiting speed; torque; power; position;
- Prevention of unexpected start-up;
- Isolation and energy dissipation function.

NOTE 1 See [Annex M](#) for additional information.

NOTE 2 Current safety research indicates that many injuries occur due to SRP/CS being defeated or circumvented. Therefore, the design of the SRP/CS should carefully take maintenance considerations into account.

The incentive to defeat or circumvent risk reduction measures provided by the SRP/CS during maintenance of the machine shall be considered when designing and selecting the SRP/CS.

NOTE 3 The incentive, or necessity, to defeat or circumvent the SRP/CS depends on both the circumstances considered and the design details of the risk reduction measure(s). Incentives to defeat or circumvent a risk reduction measure can include but are not limited to factors such as

- a) the risk reduction measure prevents the task from being performed;
- b) there is a need to perform a task that was not identified and assessed for hazards and risks;
- c) the risk reduction measure slows down production or interferes with any other activities or preferences of the user;
- d) the risk reduction measure is difficult to use;
- e) additional personnel other than the intended operator(s) perform the task, e.g.:
 - a) operator performs reset and restart functions while maintenance personnel are inside the hazard zone;
 - b) risk reduction measures intended to protect an individual are inappropriately used for multiple personnel;
- f) the risk reduction measure and/or its associated hazard is not recognized as such by personnel;
- g) the risk reduction measure is not accepted as suitable, necessary or appropriate for its function.

NOTE 4 The use of programmable systems introduces an additional possibility to defeat or circumvent provisions for access to programmable systems if not properly applied or supervised. This is particularly important when remote access for diagnostic or process correction purposes is required.

When a machine is capable of remote access for diagnostic or process correction purposes, the SRP/CS shall be designed to remain operational unless other risk reduction measures are used to maintain risk at an acceptable level.

The design of the SRP/CS shall prevent a remote restart of the machine without appropriate notification or indication to persons that are at or near the machine.

NOTE 5 A remote restart 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 to be carried out by an SRP/CS, a required performance level (PL_r) shall be determined and documented. The determination of the required performance level shall be based on the result of the risk assessment and shall correlate to the amount of the risk reduction to be carried out by the SRP/CS (see [Figure 3](#)). The required performance level for each safety function shall be determined by an estimation of the risk. The informative [Annex A](#) provides guidance for the determination of the PL_r for the safety function.

Because the methodology for determining the required performance level includes subjective estimations, some variability is acceptable in the practical application of particular cases

NOTE The PL_r for a safety function determines the reliability of the control system to execute the safety function and 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 requirement specification

The safety requirements specification shall be verified before starting the design, since every other activity is based on these requirements. The review shall ensure that all safety functions are specified to achieve the intended risk reduction at the machine.

NOTE Depending on the specific safety functions it can be useful to have independence between who prepares the SRS and who reviews it.

6 Design considerations

6.1 Evaluation of the achieved performance level PL

6.1.1 General overview of Performance level PL

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

A Performance Level shall be determined for each subsystem and/or each combination of subsystems that provide a safety function. The PL of the subsystem shall be determined by the estimation of the following aspects:

- 1) the architecture (see [6.1.3](#));
 - a) assign a category to the subsystem and evaluate the result;
 - b) evaluate if the applicable qualitative (non-quantifiable) requirements of the category are met, including:
 - Basic safety principles (see ISO 13849-2:2013, Table A.1, Table B.1, Table C.1 and Table D.1);
 - Well-tried safety principles (see ISO 13849-2:2013, Table A.2, B.2, C.2 and D.2);
 - Well-tried components (see ISO 13849-2:2013, Table A.3 and Table D.3, Annex B and Annex C);
 - c) evaluate that required behaviour under fault condition(s) is met;
- 2) the MTTF_D value for single components (see [6.1.4](#), [Annex C](#) and [Annex D](#));
- 3) the DC (see [6.1.5](#) and [Annex F](#));
- 4) the CCF (see [6.1.6](#) and [Annex F](#));

- 5) the effect of the safety related software design on the operation of the hardware (see [Clause 7](#) and [Annex J](#));
- 6) 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 certain influence.

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

- a) quantifiable aspects (MTTF_D value for single components, DC, CCF, architecture);
- b) 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 2 The contribution of reliability (e.g. MTTFD, architecture) can vary with the safety-related parts used. For example, it is possible (within certain limits) for a single channel of safety-related parts of high reliability to provide the same or higher PL as a fault-tolerant architecture of lower reliability.

NOTE 3 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. IEC 61508, IEC 61078).

To make the assessment of the PL easier, this part of ISO 13849 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](#)), [6.1.9](#), using the procedure given in [Annex B](#) to [Annex H](#), [Annex J](#), [Annex K](#) and [Annex L](#).

For PL evaluation of subsystem combinations see [6.2](#).

The achievement of qualitative aspects of the PL and the avoidance of systematic failures can be demonstrated by the application of the measures throughout this document and in [Annex G](#).

Risk reduction measures shall be applied, principally the following:

- 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 well-tried components and/or applying well-tried safety principles, in order to minimize or exclude critical faults or failures (see ISO 13849-2).
- Improve the structure of the subsystem. The aim is to avoid the dangerous effect of a fault. Some faults may be detected and a redundant and/or monitored structure could be needed.

Both measures can be applied separately or in combination. With some technologies, risk reduction can be achieved by selecting reliable components and by fault exclusions; but with other technologies, risk reduction could require a redundant and/or monitored system. In addition, common cause failures (CCF) shall be taken into account.

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](#).

It is not necessary to determine DC, MTTF, CCF and to evaluate SRESW for subsystems, which already have PL or SIL, and PFH_D-value from manufacturer.

6.1.2 Correlation between PL and SIL

When a safety function is designed using one or more subsystem, each subsystem shall be designed either using PLs according to this part of ISO 13849, or using SILs according to IEC 62061/IEC 61508 (see also ISO/TR 23849). Subsystems designed according to IEC 61508 or IEC 62061 may be used but shall be restricted to those designed for high demand or continuous mode that use Route 1H (see IEC 61508-2:2010, 7.4.4.2). Subsystems are to be combined according to 6.2. See Table 3 for correlations between PLs and SILs.

Table 3 — Correlation between performance level (PL) and safety integrity level (SIL)

PL	SIL
	(IEC 62061, for information) high/continuous mode of operation
a	No correlation
b	1
c	1
d	2
e	3

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

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, DC_{avg} and CCF

6.1.3.1 General

The SRP/CS or subsystem designed according to this part of ISO 13849 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 state The Categories describe the required behaviour of the subsystem in respect of its resistance to faults based on the design considerations described in Clause 4.

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 fault tolerance and/or diagnostic measures. In category 2 this is provided by periodically checking that the specified safety function is being performed correctly (without faults). In categories 3 and 4 this is provided by ensuring that the single fault will not lead to the loss of the safety function. In category 4, and whenever reasonably practicable in category 3, such faults will be detected. Table 4 gives an overview of categories of the subsystem, the requirements and the system behaviour in case of faults.

Table 4 — Overview of requirements for categories

Category	Summary of requirements	System behaviour	Principle used to achieve safety	MTTF _D of each functional channel	DC _{avg}	CCF
B (see 6.1.3.2.2)	Subsystem and/or their protective equipment, 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 safety 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-tried components and well-tried safety principles shall be used.	The occurrence of a fault can lead to the loss of the safety 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-tried safety principles shall apply. Safety function shall be checked at suitable intervals by the machine control system (see 6.1.8).	The occurrence of a fault can lead to the loss of the safety function between the checks. The loss of safety function is detected by the check.	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-tried safety principles shall apply. Safety-related parts shall be designed, so that — a single fault in any of these parts does not lead to the loss of the safety function, and — whenever reasonably practicable, the single fault is detected.	When a single fault occurs, the safety function is always performed. Some, but not all, faults will be detected. Accumulation of undetected faults can lead to the loss of the safety function.	Mainly characterized by structure	Low to high	Low to medium	See Annex F
NOTE For full requirements, see 6.1.3.2 .						

Table 4 (continued)

Category	Summary of requirements	System 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. Safety-related parts shall be designed, so that — a single fault in any of these parts does not lead to a loss of the safety function, and — the single fault is detected at or before the next demand upon the safety function, but that if this detection is not possible, an accumulation of undetected faults shall not lead to the loss of the safety function.	When a single fault occurs the safety function is always performed. Detection of accumulated faults reduces the probability of the loss of the safety function (high DC). The faults will be detected in time to prevent the loss of the safety function.	Mainly characterized by structure	High	High including accumulation of faults	See Annex F
NOTE For full requirements, see 6.1.3.2 .						

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

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

- the reduction in risk to be achieved by the safety function to which the part contributes,
- the required performance level (PL_r),
- the technologies used,
- the risk arising in the case of a fault(s) in that part,
- the possibilities of avoiding a fault(s) in that part (systematic failure),
- the mean time to dangerous failure (MTTF_D),
- the diagnostic coverage (DC), and
- the common cause failure (CCF) 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 typically meet the requirements of the respective category.

[Figure 7](#) to [Figure 11](#) do not show examples but general 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), such that the system meets the required performance level (PL_r).

For a subsystem which deviates from the designated architectures, a detailed calculation shall be provided to demonstrate the achievement of the required performance level (PL_r).

The designated architectures show a logical representation of the structure of the subsystems for each category. For categories 3 and 4, this means that not all parts are necessarily physically redundant but that there are redundant means of assuring that a single fault cannot lead to the loss of the safety function. Therefore, the technical realization (for example, the circuit diagram) can differ from the logical representation of the architecture.

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

NOTE 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 which 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 [Figure 12](#) is used to estimate the PL, the architecture of the subsystem shall be equivalent to the designated architecture of the claimed category. Designs fulfilling the characteristics of the respective category in general are equivalent to the respective designated architecture of the 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 ISO 13849-2) 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, power supply interruptions or disturbances.

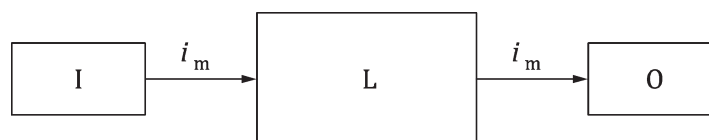
NOTE 1 There is no diagnostic coverage ($DC_{avg} = \text{none}$) within category B systems. In such structures, the consideration of CCF is not relevant.

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

The maximum PL achievable with category B is $PL = b$.

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

Specific requirements for electromagnetic compatibility (EMC) (immunity requirements) are found in the relevant product or generic standards. Immunity requirements are particularly relevant for subsystems. SRP/CS containing active electronic components shall meet EMC 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