
**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

STANDARDSISO.COM : Click to view the full PDF of ISO 13849-1:2023



STANDARDSISO.COM : Click to view the full PDF of ISO 13849-1:2023



COPYRIGHT PROTECTED DOCUMENT

© ISO 2023

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
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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.

STANDARDSISO.COM : Click to view the full PDF of ISO 13849-1:2023

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

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 subsystems	6.2
PL _r	required performance level	3.1.6
r _d	demand rate	3.1.38
r _t	test rate	3.1.37
RDF	ratio of dangerous failures	3.1.34
RS	rotation sensor	Annex I

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

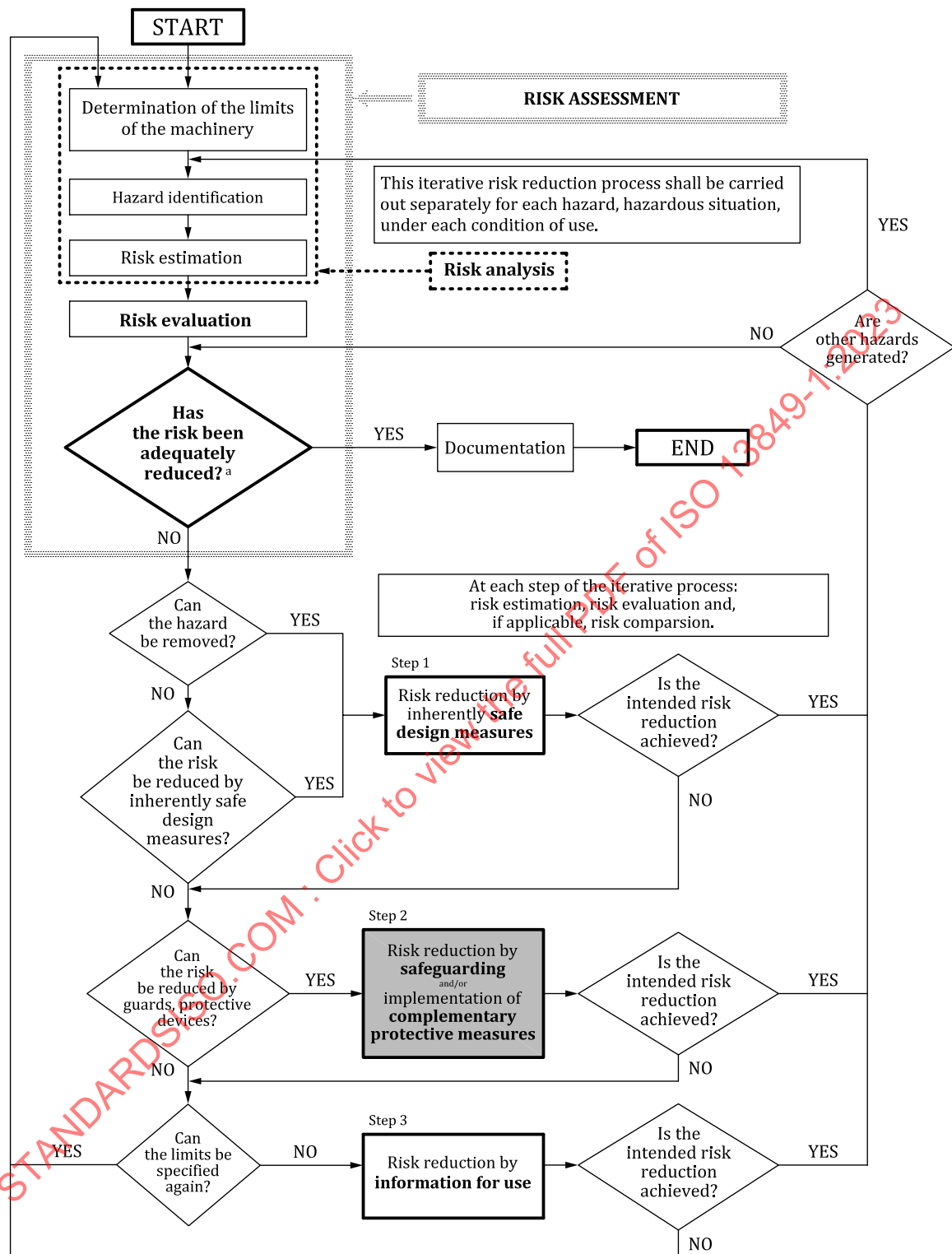
4.1 Risk assessment and risk reduction process at the machine

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.

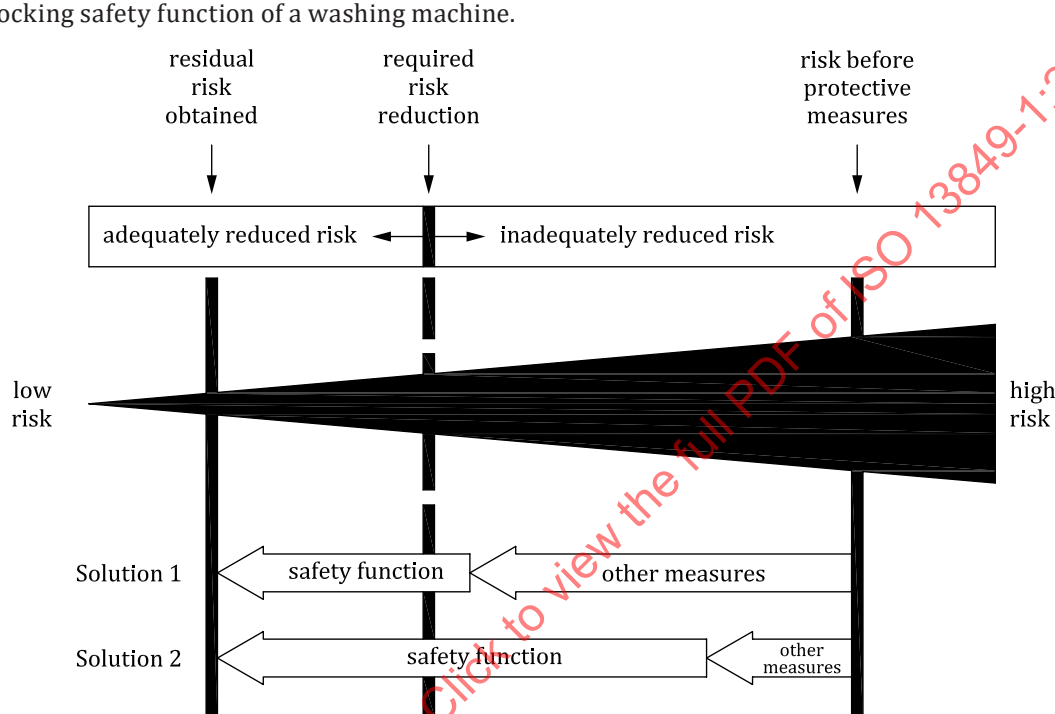
Figure 2 — Schematic representation of risk reduction process including iterative three-step method

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.

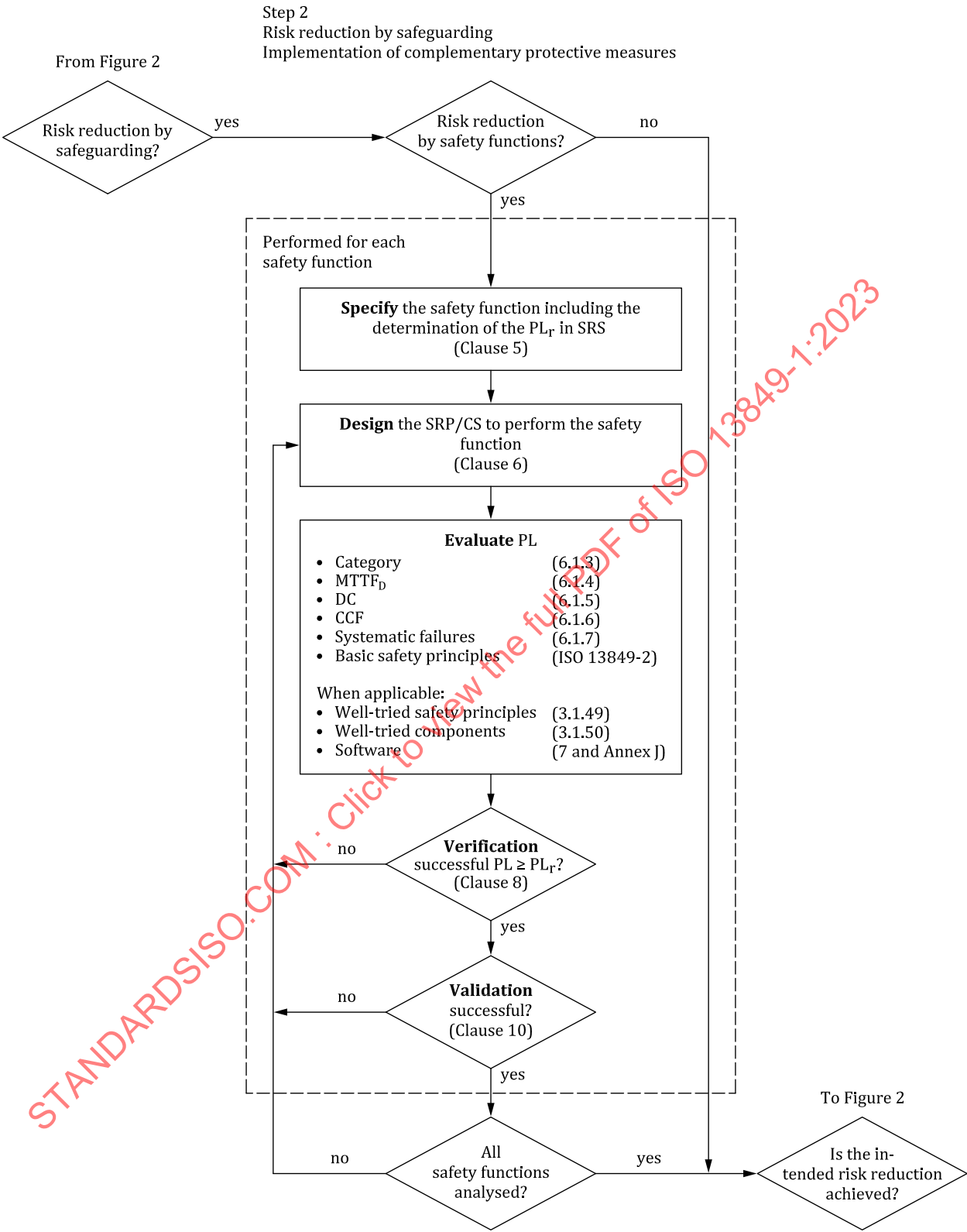


Figure 4 — Iterative process for design of safety-related parts of control systems (SRP/CS)

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](#)).

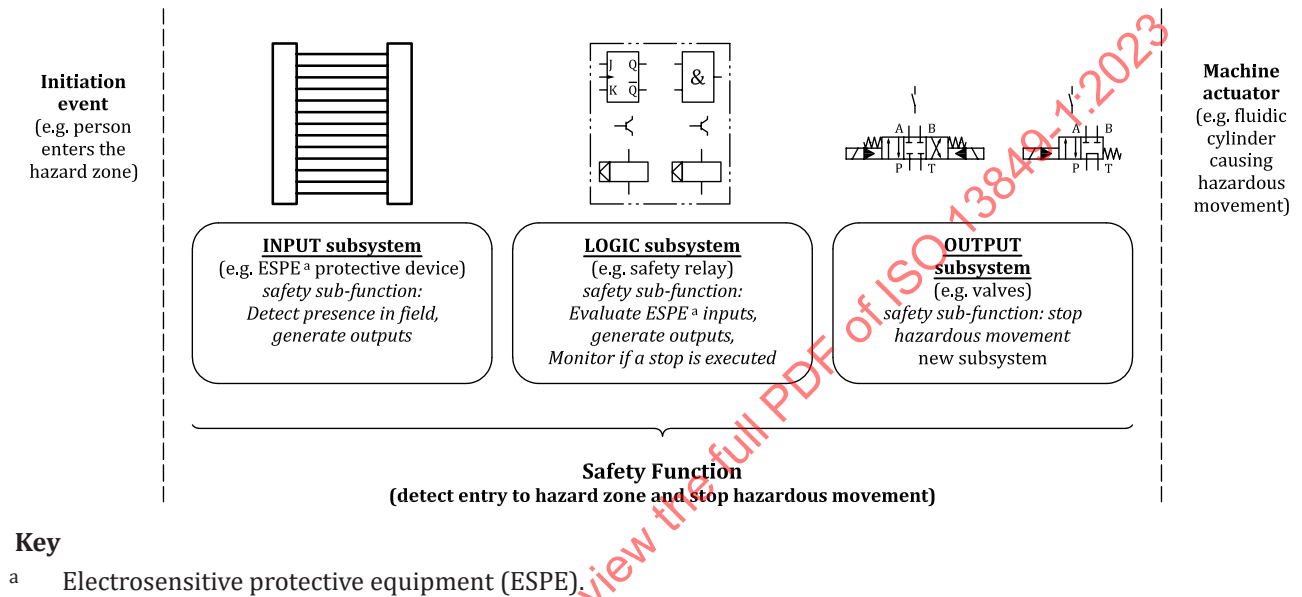


Figure 5 — Example of combination of subsystems

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

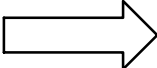
5.2.1.1 General

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](#)).

STANDARDSISO.COM : Click to view the full PDF of ISO 13849-1:2023

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_{rd} — 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_{rc} — 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.

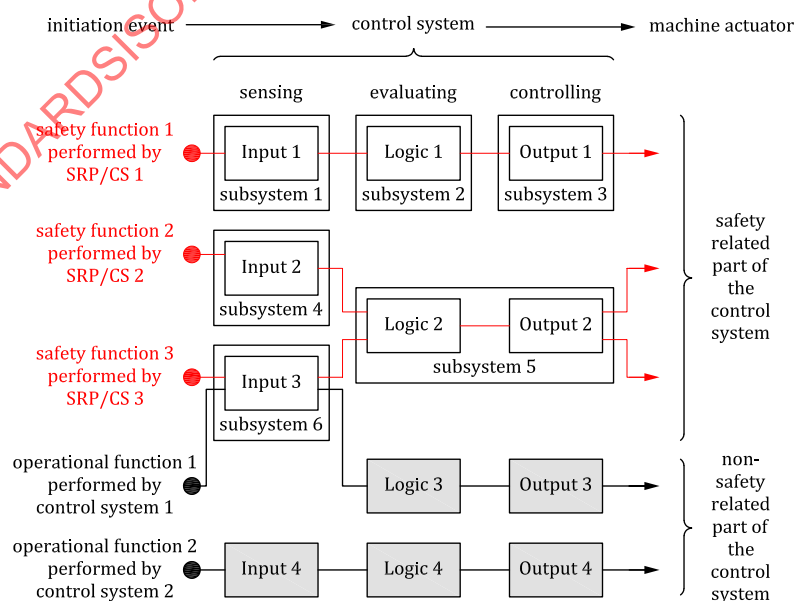


Figure 6 — Example of decomposition of safety functions and their allocation to subsystems

[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. Subsystem 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),
- 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.

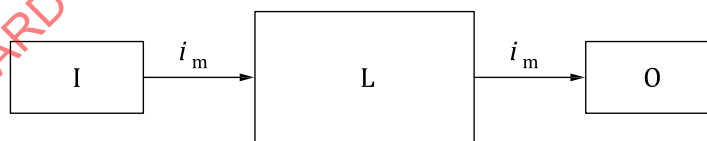
The $MTTF_D$ of the channel shall be at least low.

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

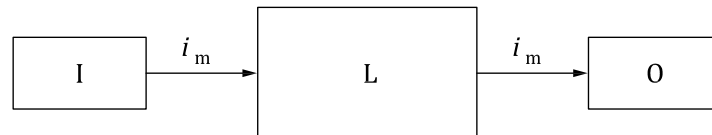
For category 1, the same requirements as those according to [6.1.3.2.2](#) for category B shall apply. In addition, the following applies.

Subsystems of category 1 shall be designed and constructed using well-tries components according to 6.1.11 and well-tries 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-tries 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 $PL_{r,c}$, 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).

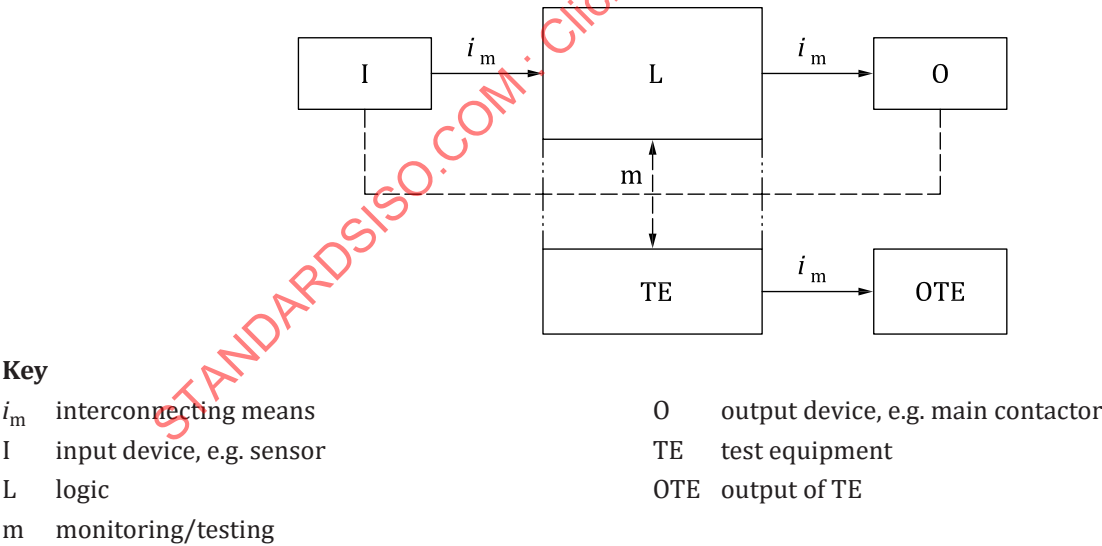
The maximum PL achievable with category 2 is PL d.

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.



The dashed lines represent reasonably practicable fault detection.

Figure 9 — Designated architecture for category 2

6.1.3.2.5 Category 3

For category 3, the same requirements as those according to 6.1.3.2.2 for category B shall apply. Well-tried safety principles according to 3.1.49 and ISO 13849-2:2012 shall also be followed. In addition, the following applies.

The maximum PL achievable with category 3 is PL e.

Subsystems of category 3 shall be designed so that a single fault does not lead to the loss of the sub-function. Whenever reasonably practicable, the single fault shall be detected at or before the next demand upon the safety function.

The DC of the total subsystem shall be at least low. The $MTTF_D$ of each of the redundant channels shall be low-to-high, depending on the PL_r . Measures against CCF shall be applied (see Annex F).

NOTE 1 The requirement of single-fault detection does not mean that all faults will be detected. Consequently, the accumulation of undetected faults can lead to an unintended output and a hazardous situation at the machine. Typical examples of practicable measures for fault detection are use of the feedback of mechanically guided relay contacts and monitoring of redundant electrical outputs (see Annex E).

NOTE 2 If necessary, because of technology and application, type-C standard makers can give further details on the detection of faults.

NOTE 3 Category 3 subsystem behaviour is characterized by

- continued performance of the sub-function in the presence of a single fault,
- detection of some, but not all, faults, and
- possible loss of the sub-function due to accumulation of undetected faults.

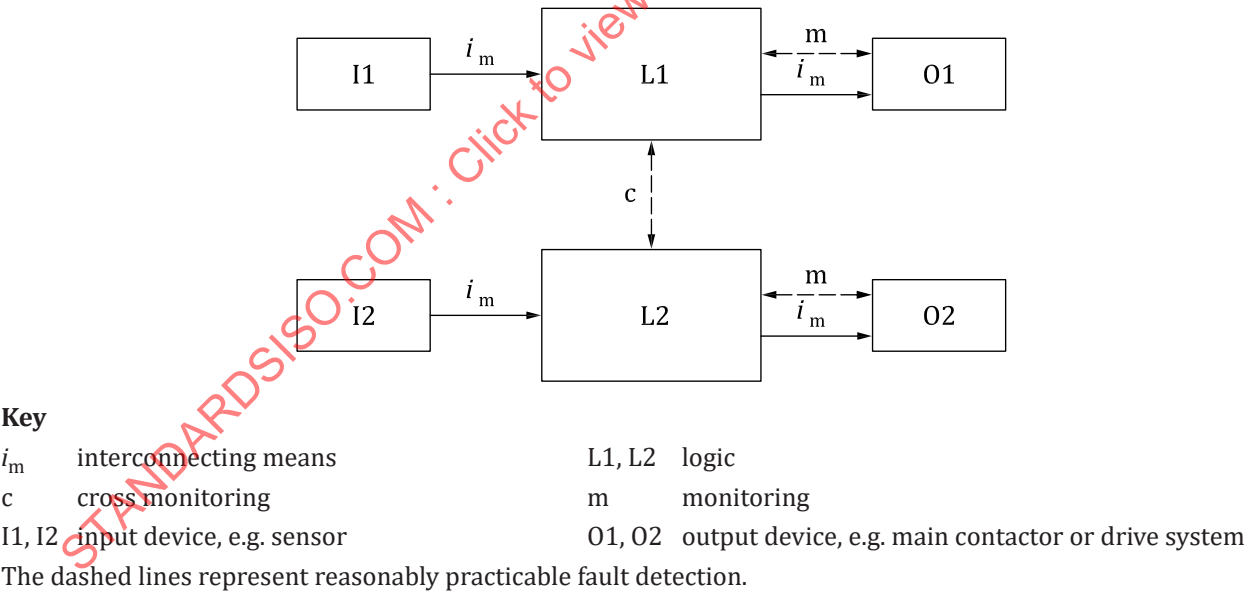


Figure 10 — Designated architecture for category 3

6.1.3.2.6 Category 4

For category 4, the same requirements as those according to 6.1.3.2.2 for category B shall apply. Well-tried safety principles according to 3.1.49 and ISO 13849-2:2012 shall also be followed. In addition, the following applies.

The maximum PL achievable with category 4 is PL e. Subsystem of category 4 shall be designed such that

- a single fault 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 functions, e.g. immediately, at switch on, or at the end of a machine operating cycle but if this detection is not possible, then an accumulation of undetected faults shall not lead to the loss of the safety function.

NOTE 1 Based on an analysis, e.g. FMEA, undetected failures with a very low probability do not need to be considered for accumulation of faults if this is documented and verified.

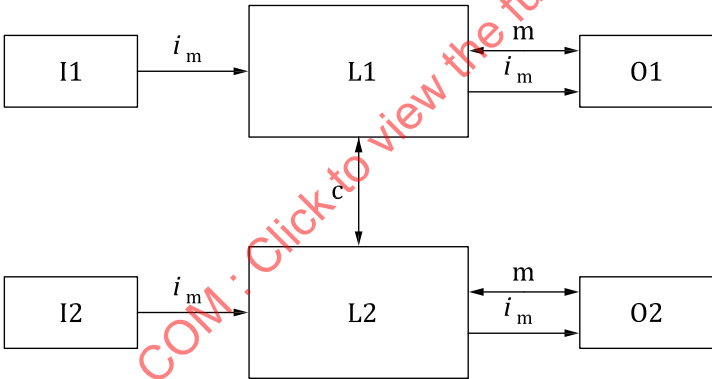
The average diagnostic coverage (DC_{avg}) of the total subsystem shall be high. The $MTTF_D$ of each of the redundant channels shall be high. Measures against CCF shall be applied (see Annex F).

NOTE 2 Category 4 system behaviour is characterized by

- continued performance of the safety function in the presence of a single fault,
- detection of faults in time to prevent the loss of the safety function, and
- the accumulation of undetected faults being taken into account.

NOTE 3 The difference between category 3 and category 4 is a higher DC_{avg} in category 4 and a required $MTTF_D$ of each channel of “high” only.

In practice, the consideration of a fault combination of two faults can be sufficient.



Key

i_m	interconnecting means	L1, L2	logic
c	cross monitoring	m	monitoring
I1, I2	input device, e.g. sensor	O1, O2	output device, e.g. main contactor or drive system

Solid lines for monitoring (m) represent DC that is higher than in the designated architecture for category 3.

Figure 11 — Designated architecture for category 4

6.1.4 Mean time to dangerous failure ($MTTF_D$)

The mean time to dangerous failure ($MTTF_D$) is a quantity with the dimension of time to characterize the basic reliability of the components used. Given a constant dangerous failure rate, the $MTTF_D$ is reciprocal of the dangerous failure rate (e.g. with failures in 10^9 hours converted into years between failures).

For the estimation of $MTTF_D$ of a component, the order of priorities is:

- a) use manufacturer’s data;

NOTE 1 When $MTTF_D$ data of components (e.g. electromechanical components) are provided by the manufacturer, the number of operations indicated by the manufacturer is considered so that the number of operations in the real application is not higher than the number of operations indicated by the manufacturer.

- b) use methods in [Annex C](#);
- c) failure rate field data from identical component applications in similar environments collected over a significant period of time and where the collection and analysis method results in a reasonable level of confidence in the data;

NOTE 2 Further information about field data is detailed in IEC 61508-7:2010, B.5.4.

- d) choose 10 years.

[Annex C](#) gives practical guidance on how to calculate or evaluate $MTTF_D$ values for single components. [Annex D](#) describes how to derive the $MTTF_D$ of each channel from this, including parts-count method and symmetrisation.

For each subsystem according to [Table 5](#), the maximum value of $MTTF_D$ for each channel is limited to 100 years. For category 4 subsystems, the maximum value of $MTTF_D$ for each channel is limited to 2 500 years.

NOTE 3 This higher value is justified because in category 4 the other quantifiable aspects, structure and DC, are at their maximum point and this allows the series combination of more than 3 subsystems with category 4 to achieve PL e in accordance with [6.2](#).

The value of the $MTTF_D$ of each channel is given in three levels (see [Table 6](#)) and shall be taken into account for each channel (e.g. single channel, each channel of a redundant system) individually.

Table 6 — Mean time to dangerous failure ($MTTF_D$) of each channel

$MTTF_D$	
Denotation of each channel	Range of each channel
low	$3 \text{ years} \leq MTTF_D < 10 \text{ years}$
medium	$10 \text{ years} \leq MTTF_D < 30 \text{ years}$
high	$30 \text{ years} \leq MTTF_D \leq 100 \text{ years}^a$
NOTE 1 The choice of the $MTTF_D$ ranges of each channel is based on failure rates found in the field as state-of-the-art, forming a kind of logarithmic scale fitting to the logarithmic PL scale. An $MTTF_D$ value of each channel less than three years is not expected to be found for real subsystems since this would mean that after one year about 30 % of all systems on the market will fail and will need to be replaced. An $MTTF_D$ value of each channel greater than 100 years is not acceptable because subsystems for high risks should not depend on the reliability of the components alone. To reinforce the subsystems against systematic and random failure, additional means such as redundancy and testing are necessary. To be practicable, the number of ranges was restricted to three. The limitation of $MTTF_D$ of each channel to a maximum of 100 years refers to the single channel of the subsystem which carries out the safety function. Higher $MTTF_D$ values can be used for single components (see Table D.1). NOTE 2 The indicated limit values of this table are assumed within an accuracy of 5 %. ^a For Category 4, the $MTTF_D$ is limited to 2 500 years.	

6.1.5 Diagnostic coverage (DC)

Diagnostic coverage (DC) is determined as the ratio between rate of detected dangerous failures and the rate of total dangerous failures. DC shall be considered in categories 2, 3 and 4.

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{Dtotal}} \quad (1)$$

where

$\sum \lambda_{DD}$ is the sum of all failure rates of detected dangerous failures;

$\Sigma \lambda_{Dtotal}$ is the sum of all failure rates of total dangerous failures.

DC shall be based on either failure modes and effects analysis (FMEA) (see IEC 60812:2018), or by using simplified estimation of DC based on [E.1](#) and [Table E.1](#). [E.2](#) describes how the average diagnostic coverage (DC_{avg}) can be estimated.

NOTE 1 For the estimation of DC, in most cases, FMEA (see IEC 60812 and EN 50495:2010, Annex B) or similar methods can be used to consider either all relevant faults or failure modes, or both. See also ISO 13849-2:2012, E.5.3.

NOTE 2 Often logic units take care of diagnostic functions of input and output device.

NOTE 3 The used technology will influence the possibilities for the implementation of fault detection.

The value of the DC is given in four levels as shown in [Table 7](#).

Table 7 — Diagnostic coverage (DC)

Denotation	DC
	Range
none	$DC < 60 \%$
low	$60 \% \leq DC < 90 \%$
medium	$90 \% \leq DC < 99 \%$
high	$99 \% \leq DC$

NOTE 1 For subsystems consisting of several parts an average value DC_{avg} for DC is used in [Figure 12](#), [Clause 7](#) and [E.2](#).

NOTE 2 The choice of the DC ranges is based on the key values 60 %, 90 % and 99 % also established in other standards dealing with DC of tests. Investigations show that $(1 - DC)$ rather than DC itself is a characteristic measure for the effectiveness of the test. $(1 - DC)$ for the key values 60 %, 90 % and 99 % forms a kind of logarithmic scale fitting to the logarithmic PL scale. A DC value less than 60 % has only a slight effect on the reliability of the tested system and is therefore called "none". A DC value greater than 99 % for complex systems is very hard to achieve. To be practicable, the number of ranges was restricted to four. The indicated limited values of this table are assumed within an accuracy of 5 %.

6.1.6 Common cause failures (CCFs)

The probability of two or more separate faults having a common cause shall be taken into account for subsystems of category 2, 3 and 4. In category 2 CCF refers to common cause failures in the functional channel and the testing channel. In category 3 and 4, CCF refers to common cause failures in both functional channels. Sufficient measures against CCF shall be carried out (for guidance, see [Annex F](#)).

6.1.7 Systematic failures

Systematic failures occur for a variety of reasons, including, e.g.:

- wrong design specifications;
- manufacturing failures;
- environmental stress effects (e.g. temperature, vibration and EMI immunity);
- operational failures;
- human errors in the SRS, design of hardware and software.

To establish a sufficient level of systematic integrity, the approach to design and implement safety functions shall be systematic.

Activities that are necessary for the achievement of the required functional safety of the SRP/CS shall be documented in a functional safety plan. The functional safety plan is intended to provide measures for preventing incorrect specification, implementation, or modification issues.

In the design process especially, control and avoidance of systematic failures shall be implemented (see [Clause 10](#) and [Annex G](#)).

6.1.8 Simplified procedure for estimating the performance level for subsystems

This subclause describes a simplified procedure for estimating the PL of a subsystem based on designated architectures. Other architectures may be mapped to these designated architectures in order to obtain an estimation of the PL (see [6.1.1](#)).

The designated architectures are represented as block diagrams and are listed in the context of each category in [6.1.3.2](#). Information about the block method and the safety-related block diagrams are given in [6.1.3.2](#) and [Annex B](#). See also IEC 61078:2016.

A designated architecture is always assigned to a subsystem. In case the SRP/CS consists of one subsystem, the designated architecture will be the same for the entire SRP/CS. In case the SRP/CS consists of multiple subsystems, every subsystem shall be assigned a designated architecture, so a single SRP/CS can comprise multiple architectures.

The simplified approach is based on:

- a) mission time (T_M), 20 years (see [3.1.36](#));
- b) constant failure rates within the mission time;
- c) sufficient measures to prevent CCF have been applied (beta factor of 2 %). For guidance see [Annex F](#) or IEC 61508-6:2010, Annex D.

NOTE The mission time (T_M) is assumed to be 20 years, within which the component reliability by constant failure rates can be described or approximated. This is generally accomplished in electronic subsystems. The SRP/CS is replaced when the mission time has been reached or equivalent measures are performed to ensure that the estimated PL is still valid.

In order to claim a mission time of 20 years, the requirements according to [6.1.3.2.2](#) for Category B shall be observed. The actual mission time may be less than 20 years when using components which wear out sooner or for other technical reasons which should be documented. See also [C.4](#).

The methodology considers the categories as architectures with defined DC_{avg} . The PL of each subsystem depends on the architecture, the $MTTF_D$ in each channel and the DC_{avg} .

For a subsystem with software, the requirements of [Clause 7](#) shall be applied. The combination of several subsystems is considered in [6.2](#).

[Figure 12](#) shows which selection of categories in combination with the $MTTF_D$ of each channel and DC_{avg} is able to achieve the PL. For the estimation of the PL, [Figure 12](#) gives the different possible combinations of category with DC_{avg} (horizontal axis) and the $MTTF_D$ of each channel (columns). The columns in the diagram represent the three $MTTF_D$ ranges of each channel (low, medium and high) which can be selected to achieve the required PL.

Before using this simplified approach with [Figure 12](#) (which represents results of different Markov models based on designated architectures of [6.1.3](#)), the category of the subsystem (see [6.1.3.2](#)) as well as DC_{avg} (see [6.1.5](#)) and the $MTTF_D$ of each channel (see [6.1.4](#)) shall be determined (see [Annex C](#) to [Annex E](#)). For categories 2, 3 and 4, sufficient measures against CCF shall be carried out (for guidance, see [6.1.6](#) and [Annex F](#)). Taking these parameters into account, [Figure 12](#) provides a graphical method for determining the PL, achieved by the subsystem. The combination of category (including CCF) and DC_{avg} determines which column of [Figure 12](#) is to be chosen. According to the $MTTF_D$ of each channel, one of the three different shaded areas of the relevant column shall be chosen.

The vertical bands in [Figure 12](#) show the range of performance that can be expected from each combination of $MTTF_D$, Category and DC_{avg} . Finding the appropriate ranges for each of these variables in the bands in the [Figure 12](#) and then reading across to the vertical axis will indicate the PL that can be

achieved with this combination. For a more precise numerical selection of PL depending on the precise value of $MTTF_D$ of each channel, see [Annex K](#).

A detailed example of this simplified procedure for estimating the performance level for subsystems is shown in [Annex I](#).

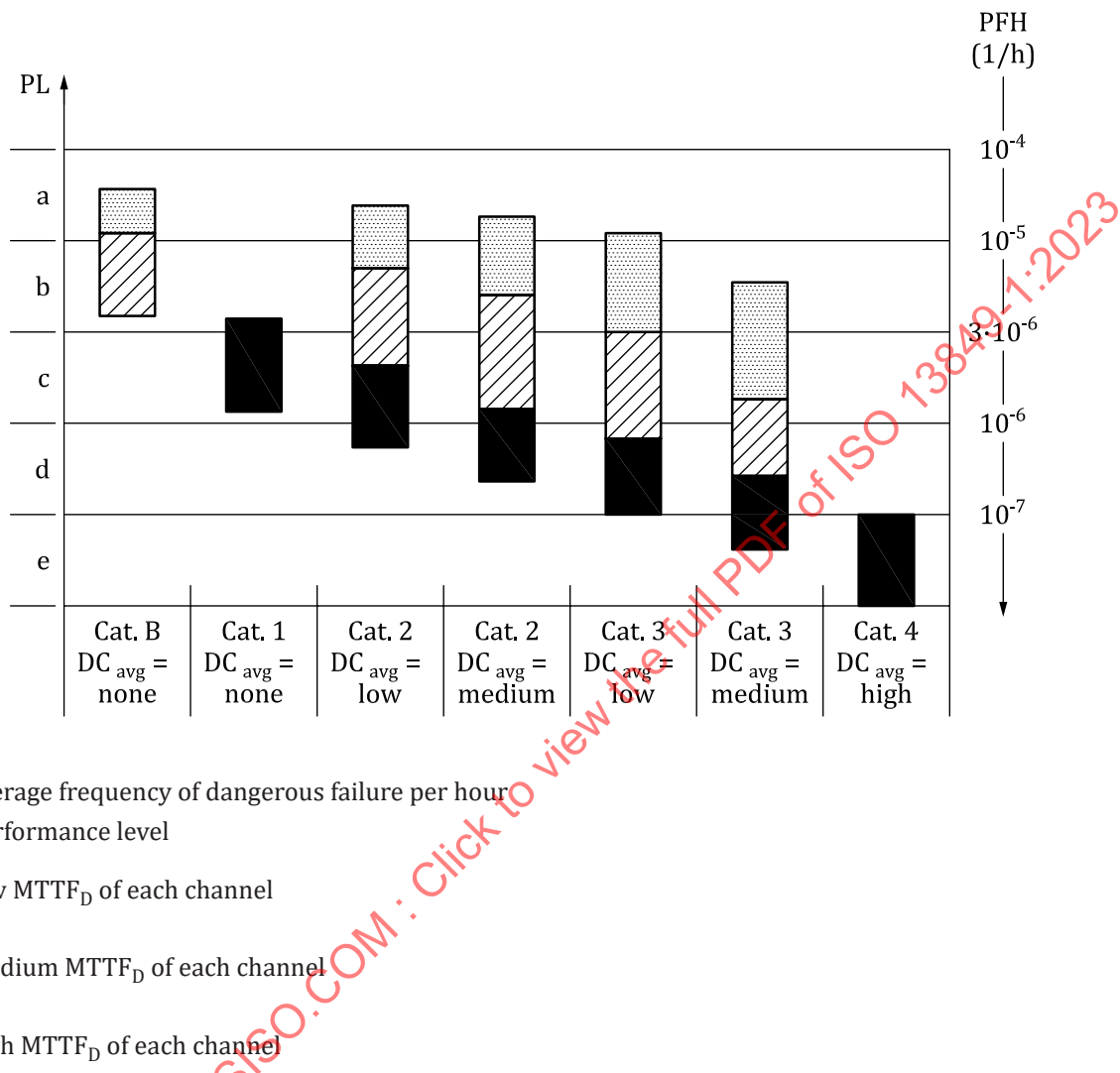


Figure 12 — Relationship between categories, DC_{avg} , $MTTF_D$ of each channel and PL

6.1.9 Alternative procedure to determine the performance level and PFH without $MTTF_D$

6.1.9.1 General

The alternative procedure to determine the PL without $MTTF_D$ is limited to subsystems incorporating mechanical, hydraulic, pneumatic, electrohydraulic or electropneumatic components where no reliability data is available and where the good engineering practice method given in [C.2](#) cannot be applied. In that case, the machine manufacturer may use the alternative procedure described in [6.1.9.2](#) to [6.1.9.4](#) to evaluate the PL without any $MTTF_D$ calculation.

The combination of several subsystems is considered in [6.2](#).

6.1.9.2 Preconditions

If for mechanical, hydraulic or pneumatic components (or components comprising a mixture of technologies) no application-specific or component manufacturer reliability data is available and the good engineering practice method of [C.2](#) cannot be applied, the machine manufacturer may evaluate the quantifiable aspects of the PL without any $MTTF_D$ calculation. Where no $MTTF_D$ data is available, the safety-related performance level (PL) can be implemented by the architecture, the DC and the measures against CCF.

As a worst case assumption the T_{10D} value is limited to 10 years. For well-tried components an assumption for T_{10D} of 20 years may be accepted. In this procedure the calculation of the DC_{avg} is reduced to the arithmetic mean value of all individual component DC values in the subsystem.

The mission time (T_M) is assumed to be 20 years. For category 2, a sufficient test rate is required (see [6.1.3.2.4](#)). The requirements, e.g. according to DC_{avg} and CCF and systematic issues, for each category (see [6.1.3](#)) shall be fulfilled.

6.1.9.3 Inputs or output subsystem

[Table 8](#) shows the relationship between achievable PL (corresponding to [Figure 12](#)) and categories. PL a and PL b can be implemented with Cat. B if basic safety principles are followed. PL c can be implemented with Cat. 1 or Cat. 2, if well-tried components, basic and well-tried safety principles are used.

PL d can be implemented with Cat. 3, respectively PL e with Cat. 4, if well-tried components, basic and well-tried safety principles are used.

Table 8 — Performance level and PFH estimation based on category and component selection

Category ^a	Additional requirements		Estimated PFH (1/h)	Achievable PL ^b
B		→	$5,0 \times 10^{-6}$	b
1		→	$1,7 \times 10^{-6}$	c
2	Only well-tried components are used	→	$1,7 \times 10^{-6}$	c
3	Only well-tried components are used	→	$2,9 \times 10^{-7}$	d
4	Only well-tried components are used	→	$4,7 \times 10^{-8}$	e
^a All requirements in 6.1.3.2.2 to 6.1.3.2.6 for the respective category shall be fulfilled, except $MTTF_D$.				
^b The achievable PL mentioned here only covers quantifiable aspects. Additional requirements for non-quantifiable aspects such as systematic failure and software (see 6.1.1) shall be fulfilled.				

6.1.9.4 Logic subsystem

Where no $MTTF_D$ data is available a conservative approach using estimated $MTTF_D$ can be assumed.

- For category B, 2 and 3 $MTTF_D$ for each channel is 10 years.
- For category 1 a $MTTF_D$ of the channel of 30 years can be assumed since well-tried components shall be used (see [6.1.3.2.3](#)).

The maximum PL that can be achieved is PL c (see [Annex K](#)).

For category 2 and category 3 common-cause failures and DC shall be considered. The DC_{avg} shall match at least 60 % for category 2 and category 3.

Category 4 is excluded in this method.

With the category, the $MTTF_D$ and the DC_{avg} , the PL and the PFH of the subsystem can be determined with [Table K.1](#).

6.1.10 Fault consideration and fault exclusion

6.1.10.1 General

When designing safety subsystems, faults and their effects shall be assessed. Each element, whose fault may cause the failure of the safety function in one of the functional channels of a subsystem, shall be considered. The designer shall make a list of faults, which can occur in the SRP/CS. This list shall include all considered faults, explanation how these faults have been noted in the design, and if fault exclusion is claimed to give reasons for these exclusions. For subsystems pre-validated by the component manufacturer, it is not necessary by the designer of the safety functions to take into account internal failures of the component(s), only failures of the interfaces.

NOTE Faults of elements, which are not directly necessary for the execution of the safety function, but which can support it (e.g. filter elements, protection against over-voltage), generally do not contribute to the MTTF_D of each channel.

6.1.10.2 Fault consideration

ISO 13849-2:2012 lists the important faults and failures for the various technologies. The lists of faults are not exhaustive and, if necessary, additional faults shall be considered and listed. In such cases, the method of evaluation shall also be clearly elaborated. For components not mentioned in ISO 13849-2:2012, a methodology to evaluate the impact of either probable faults or failures of components, or both, shall be carried out, e.g. FMEA (see IEC 60812), aiming at the identification of faults that are to be considered for those components.

In general, the following fault criteria shall be taken into account:

- if, as a consequence of a fault, further components fail, the first fault together with all following faults shall be considered as a single fault;
- the simultaneous occurrence of two or more faults having separate causes is considered highly unlikely and therefore needs not be considered.

Two or more separate faults having a common cause shall be considered as a CCF (see [Annex F](#)).

6.1.10.3 Fault exclusion

It can be necessary to exclude faults in order to evaluate subsystems. Fault exclusion is a compromise between technical safety requirements and the theoretical possibility of occurrence of a fault.

Fault exclusion can be based on

- a) the technical improbability of occurrence of some faults,
- b) generally accepted technical experience, independent of the considered application, and
- c) technical requirements related to the application and the specific hazard.

Fault exclusion is only applicable for certain failures of an element and it is up to the designer (manufacturer or integrator) to prove the exclusion of the respective faults based on the limits set forward by the design and use. Such fault exclusion is only possible provided that their unlikely occurrence can be justified based on the known laws of physical science. Any such fault exclusions shall be justified and documented.

The application of fault exclusion to certain faults for an element inside a subsystem does not limit the necessity of applying measures against systematic failures.

It is possible that some faults are excluded by the manufacturer and some by the subsystem integrator.

There shall be a specific characterization of the type of fault that is excluded. It would not be acceptable to state simply that a component will not break, distort or degrade due to wear. It is necessary to state

the direct influence under which the component will not break, distort or degrade due to wear. For example, the component will have no faults when subjected to a force of X Newtons from direction Y.

The fault exclusion shall be justifiable under all expected environmental conditions including temperature, pressure, vibration, pollution, corrosive atmosphere.

PL e shall not depend solely on fault exclusion.

NOTE 1 Information on fault exclusions is available in ISO 13849-2:2012, Annexes A to D.

NOTE 2 Product standards can give further information.

6.1.11 Well-tried component

A well-tried component for safety-related applications is a component, which shall be either

- a) widely used in the past with documented successful results in similar applications, or

NOTE See IEC 61508-2:2010, 7.4.10, for “proven in use”.

- b) listed in ISO 13849-2:2012, Annexes A to D, or

- c) made, verified and validated using principles which demonstrate its suitability and reliability for safety-related applications according to relevant product and application standards.

The decision to accept a particular component as being well-tried depends on the application, e.g. owing to the environmental influences.

Complex components (e.g. PLC, microprocessor, and application-specific integrated circuit) shall not be considered as equivalent to well-tried.

6.2 Combination of subsystems to achieve an overall performance level of the safety function

6.2.1 General

An SRP/CS may be realized using a combination of subsystems and an overall PL may be achieved using the methods described in this subclause. In this case, the validation of the combination of subsystems as an SRP/CS is required (see [Figure 13](#)). These subsystems may be assigned to one or different categories.

According to [6.1.3.2](#), the combination of subsystems to an SRP/CS starts at the points where the safety-related signals are initiated and ends at the output of the power control elements. The combined subsystems can consist of several parts connected in a linear (series alignment) way. To avoid a new complex estimation of the performance level (PL) achieved by combined subsystems where the separate PLs of all parts are already calculated, the following estimations are presented for a combination of subsystems.

If previously validated subsystems according to IEC 62061:2021 or the IEC 61508 series (SIL) for high demand or continuous mode that use Route 1_H (see IEC 61508-2:2010, 7.4.4.2) are used, the SIL can be correlated to a PL using [6.1.2](#) and [6.2.2](#). PFH values calculated according to the IEC 61508 series or IEC 62061:2021 with the above-mentioned limitations can be considered as PFH values according to this document.

Category cannot always be deduced and is not required from a subsystem validated according to IEC 62061:2021 or the IEC 61508 series.

6.2.2 Known PFH values

When combining subsystems with known PFH values, the PFH values can be combined as shown below assuming that there are n separate subsystems SB₁ to SB_n. These subsystems operate in a

series combination, which as a whole performs a safety function. For each SB_i , a PL_i has already been evaluated. This situation is illustrated in [Figure 13](#) (see also [Figure 5](#) and [Figure H.2](#)).

If the PFH values of all subsystems are known, then the PFH of the SRP/CS is the sum of all PFH values of the n individual subsystem. The PL of the SRP/CS is limited by:

- the lowest PL of any individual subsystem involved in performing the safety function, and
- the PL corresponding to the PFH of the combined SRP/CS according to [Table 2](#).

NOTE See [Annex H](#) for an example of this method.

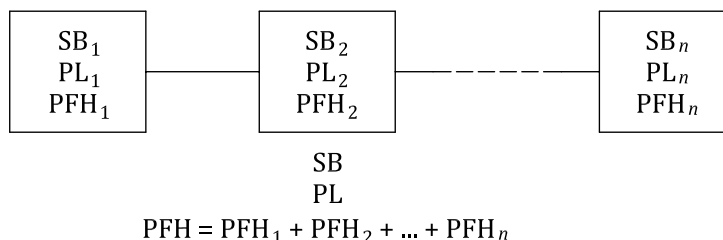


Figure 13 — Combination of subsystems to achieve overall PL

6.2.3 Unknown PFH values

If the PFH values of all individual SB_i are not known, then as an alternative to [6.2.2](#), the PL of the SRP/CS performing the safety function may be defined according to [6.2](#) or calculated using [Table 9](#) as follows:

- a) Identify the lowest PL of all subsystems: this is PL_{low} ;
- b) Identify the number of subsystems with PL_{low} : this number is N_{low} ;
- c) Look-up PL in [Table 9](#).

Table 9 — Determination of PL for series alignment of subsystems

PL_{low}	N_{low}	$\Rightarrow$	PL of the SRP/CS
a	>3	$\Rightarrow$	None, not allowed
	≤ 3	$\Rightarrow$	a
b	>2	$\Rightarrow$	a
	≤ 2	$\Rightarrow$	b
c	>2	$\Rightarrow$	b
	≤ 2	$\Rightarrow$	c
d	>3	$\Rightarrow$	c
	≤ 3	$\Rightarrow$	d
e	>3	$\Rightarrow$	d
	≤ 3	$\Rightarrow$	e

NOTE This table is based on the defined PFH ranges for each PL (see [Table 2](#)) forming a kind of logarithmic scale.

6.3 Software based manual parameterization

6.3.1 General

This subclause is limited in scope to only manual, software based parameterization that is performed and controlled by an authorized person. See also [5.2.2.6](#) and [Table M.2](#).

Some safety-related subsystems or SRP/CS need parameterization for a safety function or a sub-function.

EXAMPLE A converter with integrated sub-functions can be parameterized via a PC-based configuration tool for setting the upper speed limit parameter. To establish the detection zone of a laser scanner, parameters such as angle and distance can be configured per the manufacturer's safety documentation and the machine risk assessment.

The objective of the requirements for software based manual parameterization is to guarantee that the safety-related parameters specified for a safety function or a sub-function are correctly transferred into the hardware performing the safety function or a sub-function. Different methods can be applied to set such parameters, such as dip-switch based parameterization or dedicated parameterization software (commonly called configuration or parameterization tools).

NOTE 1 Safety-related parameterization which is carried out automatically without human interaction, for example, based on input signals, is not considered in this subclause.

NOTE 2 Direct control of a machine by an operator, e.g. speed control of a forklift truck, is not considered as manual parameterization as described in this subclause.

If the configuration or parameterization tool is pre-designed in accordance with this document or the IEC 61508 series, for example together with its dedicated subsystem, it is assumed that there will be no dangerous failures due to the influences listed in 6.3.2 or any other influence that is reasonably foreseeable. The requirements of 6.3.5 apply when a software based manual parameterization is performed with the pre-designed tool.

If a safety-related subsystem or SRP/CS is not capable of being parameterized by software based manual parameterization as described above, 6.3 does not apply.

6.3.2 Influences on safety-related parameters

Safety-related parameters shall be designed to withstand applicable external influences. During software based manual parameterization, the parameters can be affected by several influences, such as:

- a) data entry errors by the person responsible for parameterization;
- b) faults of the software of the parameterization tool;
- c) faults of further software and/or service provided with the parameterization tool;
- d) faults of the hardware of the parameterization tool;
- e) faults during transmission of parameters from the parameterization tool to the SRP/CS or a subsystem;
- f) faults of the SRP/CS or a subsystem to store transmitted parameters correctly;
- g) systematic interference during the parameterization process, e.g. by EMI or loss of power.
- h) interference due to external influences or factors, such as EMI or (random) loss of power.

With no measures applied to counteract, avoid or control potential dangerous failures caused by the influences listed above, such influence can lead to the following:

- parameters are not updated by the parameterization process, completely or in parts without notice to the person responsible for the parameterization;
- parameters are incorrect, completely or in parts;
- parameters are applied to an incorrect device, such as when transmission of parameters is carried out via a wired or wireless network.

6.3.3 Requirements for software based manual parameterization

Software based manual parameterization shall use a dedicated tool provided by the manufacturer or supplier of the SRP/CS or the related subsystem(s). The SRP/CS or the related subsystem(s) and the parameterization tool shall have the capability to prevent unauthorized modification, for example by using a dedicated password.

Parameterization while the machine is running shall be permitted only if it does not cause an unsafe state.

It is possible to fulfil the requirements by using a pre-designed subsystem.

When using a pre-designed SRP/CS or subsystem that is capable of software based manual parameterization, the target is to prevent dangerous failure due to the influences listed in 6.3.2 or any other influence that is reasonably foreseeable. The validation of the pre-designed subsystem shall include the issue of parameterization.

When an SRP/CS or subsystem that is capable of software based manual parameterization is designed according to this document there shall be no undetected dangerous failure due to the influences listed above or any other influence that is reasonably foreseeable. The following requirements shall be fulfilled in addition:

- a) The design of the software based manual parameterization shall be considered as a safety-related aspect of SRP/CS design that is described in an SRS.
- b) The SRP/CS or subsystem shall provide means to check the data plausibility, e.g. checks of data limits, format and/or logic input values.
- c) The integrity of all data used for parameterization shall be maintained. This shall be achieved by applying measures to:
 - 1) control the range of configured values by a validity (range) check;
 - 2) control data corruption before transmission;
 - 3) control the effects of errors from the parameter transmission process;
 - 4) control the effects of incomplete parameter transmission;
 - 5) control the effects of faults and failures of hardware and software of the parameterization;
 - 6) control the effect of the interruption of the power supply.
- d) The parameterization tool shall fulfil all relevant requirements for SRP/CS according to this document or the IEC 61508 series.
- e) Alternatively to d), a special procedure shall be used for setting the safety-related parameters. This procedure shall include confirmation of input parameters to the SRP/CS by either:
 - retransmitting of modified parameters to the parameterization tool; or
 - other means to confirm the integrity of the parameters;
 - as well as subsequent confirmation, for example by a suitably skilled person and by means of an automatic check by a parameterization tool. New values of safety-related parameters shall not be used for safety-related operation before the changes are acknowledged and confirmed.

NOTE This is of particular importance where a parameterization software tool uses a device not specifically intended for this purpose (e.g. personal computer or equivalent).

The software modules used for encoding/decoding within the transmission/retransmission process and software modules used for visualization of the safety-related parameters to the user shall, as a minimum, use diversity in function(s) to avoid systematic failures.

6.3.4 Verification of the parameterization tool

The following verification activities shall be performed to verify the basic functionality of the parameterization tool:

- verification of the correct setting for each safety-related parameter (minimum, maximum and representative values);
- verification that the safety-related parameters are checked for plausibility, for example by detection of invalid values;
- verification that means are provided to prevent unauthorized modification of safety-related parameters.

NOTE This is of particular importance where the parameterization is carried out using a device not specifically intended for this purpose (e.g. personal computer or equivalent).

6.3.5 Documentation of software based manual parameterization

Software based manual parameterization shall be carried out using the dedicated parameterization tool provided by the manufacturer or supplier of the SRP/CS or the related subsystem(s) and shall be documented according to the requirements given in the information for use. This information can originate from different parties, see also [Clause 13](#) (information for use). Protective measures against unauthorized access shall be activated and used.

The initial parameterization, and subsequent modifications to the parameterization, shall be documented. The documentation shall include:

- a) the date of initial parameterization or change;
- b) data or version number of the data set;
- c) name of the person carrying out the parameterization;
- d) an indication of the origin of the data used (e.g. pre-defined parameter sets);
- e) clear identification of safety-related parameters;
- f) effects and boundaries for cases where parameterization is possible or needed on a continuous basis;
- g) clear identification of the SRP/CS or associated subsystem which is subject to specific parameterization settings.

7 Software safety requirements

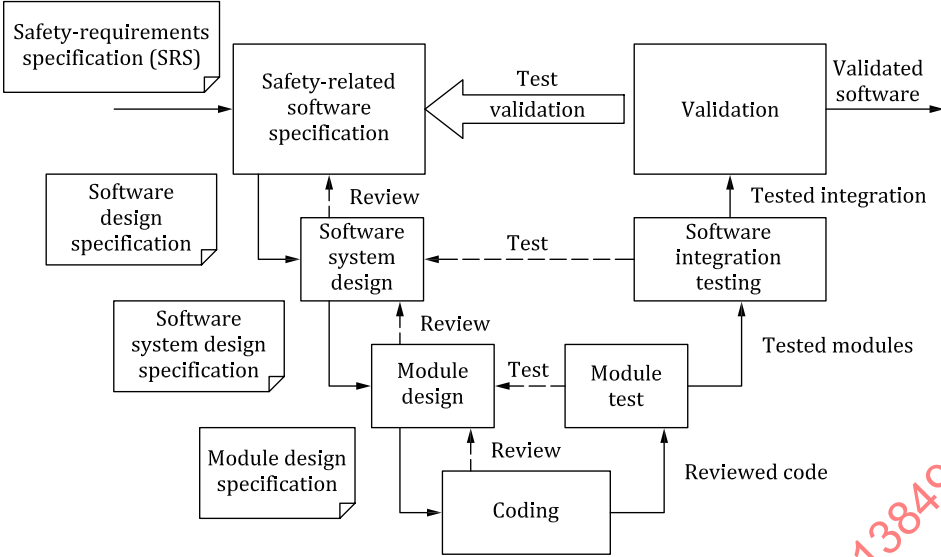
7.1 General

Although artificial intelligence (AI) can be used for SRP/CS, this clause does not address additional specific requirements necessary for AI technology and its use as part of SRP/CS.

Activities related to the development of safety-related embedded or application software shall primarily consider the avoidance of faults during the software lifecycle [see [Figure 14 a](#)]. The main objective of the following requirements is to have readable, understandable, testable and maintainable software.

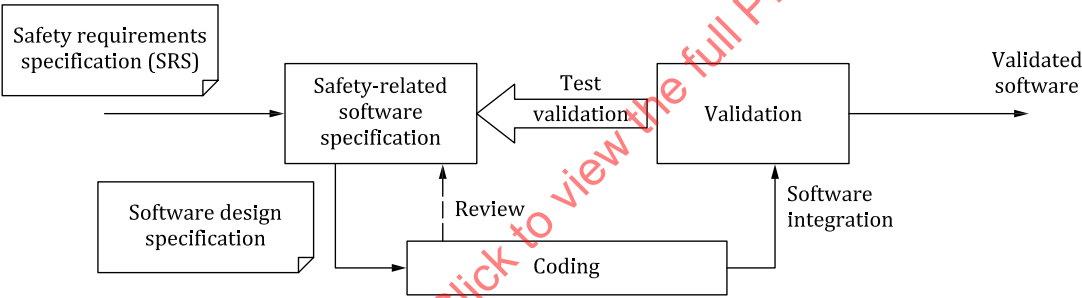
NOTE 1 [Annex I](#) gives more detailed recommendations for lifecycle activities.

NOTE 2 [Annex N](#) gives an overview of measures which apply to SRASW performed by usage of LVL and SRASW or SRESW performed by usage of FVL.



a) Simplified V-model of software safety lifecycle

If pre-assessed safety-related hardware and software modules are used in combination with LVL, a simplified software lifecycle shown in [Figure 14 b\)](#) is applicable.



b) Simplified V-model for software if pre-assessed safety-related hardware and software modules are used in combination with LVL

Key

- result
- -> verification

NOTE Typically, the simplified software lifecycle, shown in [Figure 14 b\)](#), applies to the use of module-based programming in LVL, that only require simple interconnections to be configured, which limits the inputs and outputs to a pre-defined set of values, including a combination of modules.

Figure 14 — Simplified V-model

When safety and non-safety functions are implemented in the same hardware environment, it shall be demonstrated that the safety functions are not impacted by the non-safety functions under normal or fault conditions, e.g. which may include, but is not limited to, blocking or delaying a safety response which is required to be performed at any time.

7.2 Limited variability language (LVL) and full variability language (FVL)

7.2.1 Limited variability language (LVL)

LVL is a software programming language, whose notation is textual or graphical or has characteristics of both, for commercial and industrial programmable electronic controllers with a range of capabilities limited to their application (see IEC 61508-4:2010, 3.2.14).

LVL should be designed to be easily understandable by the software designer and should be stringently focused on the applications to be implemented.

The following are examples of LVLs:

- a) ladder diagram (see IEC 61131-3:2013, 8.2): a graphical language consisting of a series of input symbols (representing behaviour similar to devices such as normally open and normally closed contacts) interconnected by lines (to indicate the flow of current) to output symbols (representing behaviour similar to relays);
- b) Function block diagram (see IEC 61131-3:2013, 8.3): in addition to Boolean operators, allows the use of more complex functions such as data transfer file, block transfer read/write, shift register and sequencer instructions;
- c) Sequential function chart (see IEC 61131-3:2013, 6.7): a graphical representation of a sequential program consisting of interconnected steps, actions and directed links with transition conditions;
- d) Boolean algebra: a low-level language based on Boolean operators such as AND, OR and NOT with the ability to add some mnemonic instructions.

7.2.2 Full variability language (FVL)

This type of language is designed for computer programmers and provides the capabilities to implement a wide variety of functions and applications. This type of language offers all possible programming options and can be used to create an application program with full flexibility in how the logic is constructed.

NOTE Typical examples of systems using FVL are general purpose computers.

In the machinery sector, FVL is found in embedded software and rarely in application software.

EXAMPLE Ada, C, Pascal, Instruction List, assembler languages, C++, Java, MATLAB, Simulink, ST and SQL (without limitations for use and full variety of instructions).

7.2.3 Decision for limited variability language (LVL) or full variability language (FVL)

In general, software can be written in FVL or LVL. The designer of the SRP/CS shall follow [Figure 15](#) for the determination, if a programming language is FVL or LVL.

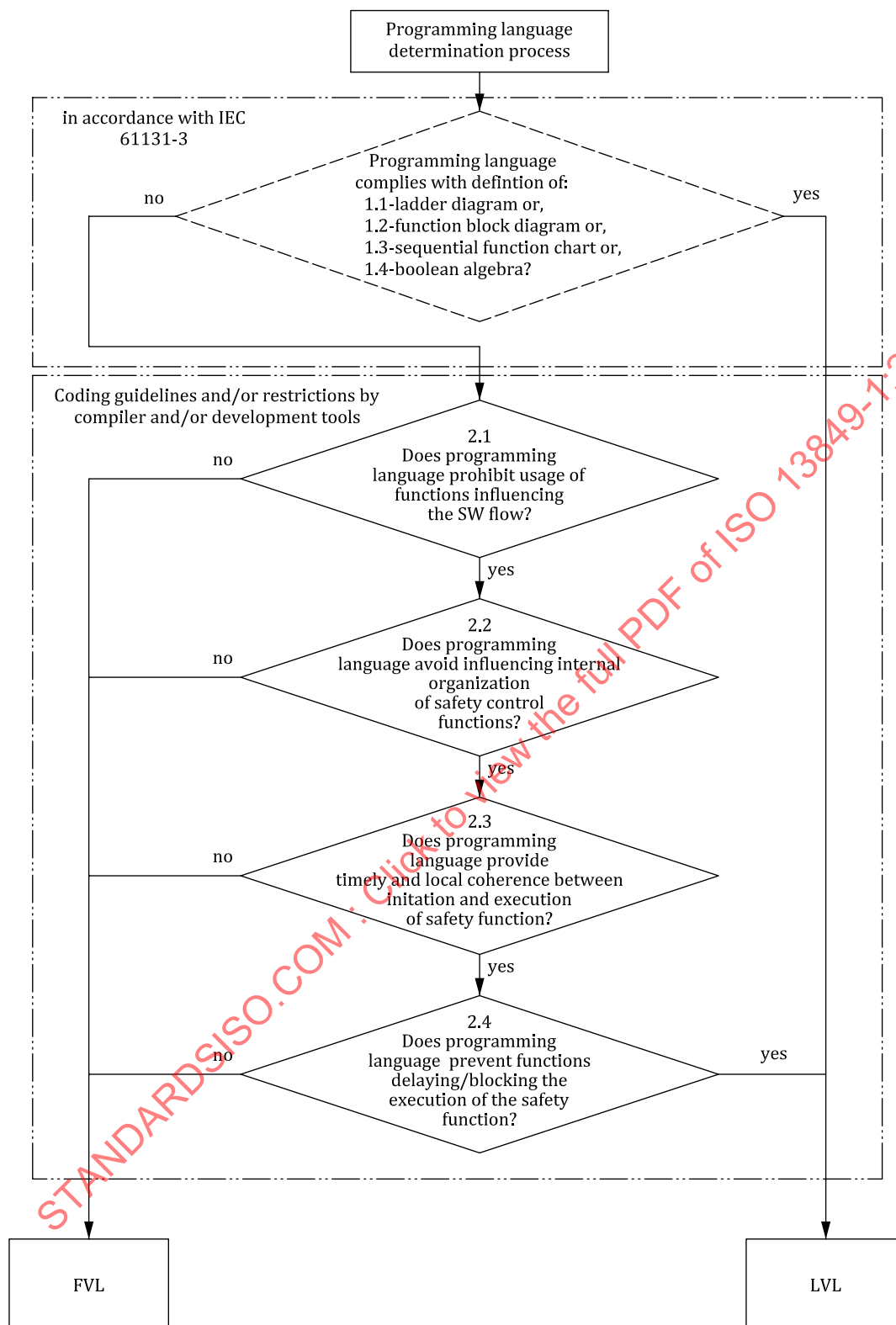


Figure 15 — Decision guideline for FVL or LVL

EXAMPLE 1 If language C is used there is no accordance with IEC 61131-3 and if any of the questions 2.1 to 2.4 in [Figure 15](#) are answered with no, the result will be FVL.

EXAMPLE 2 If a type of structured text or a limited sub-set of language C is used with restrictions within either the compiler or development tools, or both, and restrictive coding guidelines which fulfil [7.4](#) a) and b) and all of the questions 2.1 to 2.4 in [Figure 15](#) can be answered with yes, the result will be LVL.

EXAMPLE 3 If Visual Basic is used it is not in accordance with IEC 61131-3 and the questions 2.1 to 2.4 in [Figure 15](#) answered with no, the result will be FVL.

EXAMPLE 4 If the software flow is influenced by the programming language, e.g. by using interrupt (question 2.1 in [Figure 15](#)), the result will be FVL.

EXAMPLE 5 If a function block diagram is used with self-declared functions blocks in structured text in accordance with IEC 61131-3 and the restrictions of [7.4 a\)](#) and [b\)](#) are fulfilled the result will be LVL.

NOTE 1 [Annex N](#) gives an overview on the measures that apply to SRASW and SRESW performed either by usage of LVL or FVL.

NOTE 2 The technical documentation, especially safety manuals of products, can be followed for both LVL and FVL. Both limitations via internal functions of the compiler and limitations via coding guideline can be used.

7.3 Safety-related embedded software (SRESW)

7.3.1 Design of safety-related embedded software (SRESW)

For SRESW for components with PL_r a to d, the following basic measures shall be applied:

- a) software safety lifecycle with verification and validation activities, e.g. reviews and tests, see [Figure 14 a\)](#);
- b) documentation of specification and design, e.g. software design specification, software system design specification (SSDS), module design specification (MDS), code listings including comments;
- c) modular and structured design and coding, e.g. hierarchy and limitation of functionality, clear program structure, definition of interfaces, well-structured call-graph, avoidance of interrupts, use of coding guidelines (see IEC 61508-7:2010, [C.2.6.2](#));
- d) control of systematic failures, e.g. program sequence monitoring, controlling errors in the data communication process (see [G.2](#));
- e) where using software based diagnostic measures for control of random hardware failures, verification of correct implementation, e.g. correct implementation of diagnostic measures, RAM/ROM/CPU tests, hardware tests, plausibility checks;
- f) functional testing, e.g. black box testing implemented e.g. by verification of correct output data based on input data (valid, invalid and border values), compatibility of interfaces, timing;
- g) appropriate software safety lifecycle activities after modifications, e.g. based on an impact analysis.

For SRESW for components with PL_r c or d, the following additional measures shall be applied:

- h) project management and quality management processes comparable to, e.g. the IEC 61508 series, e.g. definition of workflow, responsibilities;
- i) documentation of all relevant activities during software safety lifecycle, e.g. documentation of reviews, testing, validation and verification;
- j) configuration management to identify all configuration items and documents related to a SRESW release, e.g. version control of code listings, modules, design documents, test plans, release control, archiving, system compatibility of different versions of hardware, software and programming tools;
- k) structured specification with safety requirements and structured design;
- l) use of suitable programming languages and computer-based tools with confidence from use;
- m) modular and structured programming, separation from non-safety-related software, limited module sizes with fully defined interfaces, e.g. use of design and coding guidelines;

- n) coding verification by walk-through/review with control flow analysis, e.g. to check for faults, quality of comments, conformity with coding guidelines, clarity, readability, completeness;
- o) extended functional testing, e.g. grey box testing, performance testing or simulation, e.g. by using unspecified input data, extreme environmental conditions, full load, testing based on knowledge of internal coding.

For the testing channel in Category 2, the requirements are reduced by one performance level. If diversity is used in the functional channels of Category 3 or 4, the requirements are reduced by one performance level.

SRESW for components with PL_r e shall be in accordance with IEC 61508-3:2010, Clause 7, appropriate for SIL 3. When using diversity in specification, design and coding, for the two channels used in a subsystem with category 3 or 4, PL_r e can be achieved with the above-mentioned additional measures for PL_r of c or d.

NOTE For SRESW with diversity in design and coding, for components used in a subsystem with category 3 or 4 or in testing channel of category 2, the effort involved in taking measures to avoid systematic failures can be reduced by, for example, reviewing parts of the software only by considering structural aspects instead of checking each line of code. [Annex G](#) gives guidance referring the usable measures to carry out these aspects.

7.3.2 Alternative procedures for non-accessible embedded software

When the designer of the SRP/CS is not able to access the embedded software, e.g. PLCs without safety rating by the manufacturer, the SRESW requirements of [7.3.1](#) cannot be fulfilled. These components may be used under the following alternative conditions:

- the subsystem is limited to PL a or b and uses category B, 2 or 3;
- the subsystem is limited to PL c with category 2 or PL d with category 3 and it is necessary to fulfil the diversity requirements of the CCF, where both channels use diverse technologies, design or physical principles;
- the associated hardware and the requirements for SRASW shall be assessed in accordance with the requirements of this document, especially for CCF (see [Annex F](#)).

7.4 Safety-related application software (SRASW)

The software safety lifecycle (see [7.1](#)) applies also to SRASW.

SRASW written in LVL and conforming to the following requirements can achieve a PL a to PL e. If SRASW is written in FVL, the requirements for SRESW shall apply and PL a to PL e is achievable. [Figure 15](#) shows a decision guideline for FVL or LVL.

If a part of the SRASW within one component has any impact (e.g. due to its modification) on several safety functions with different PL, then the requirements related to the highest PL shall apply.

For SRASW for components with PL_r from a to e, the following basic measures shall be applied:

- development lifecycle with verification and validation activities, e.g. reviews and tests, see [Figure 14](#) for LVL;
- documentation of specification and design;
- modular and structured programming;
- functional testing;
- appropriate development activities after modifications.

For SRASW for components with PL_r from c to e, the following additional measures with increasing efficiency (lower effectiveness for PL_r of c, medium effectiveness for PL_r of d, higher effectiveness for PL_r of e) apply.

For the testing channel in Category 2, the requirements are reduced by one performance level. If diversity is used in the functional channels of Category 3 or 4, the requirements are reduced by one performance level.

- a) The software design specification shall be reviewed (see also [Annex J](#)), made available to persons involved in the lifecycle and shall contain the description of:
 - 1) safety functions with required PL and associated operating modes;
 - 2) performance criteria, e.g. reaction times;
 - 3) communication interfaces;
 - 4) detection and control of hardware failures to achieve the required DC and fault reaction.
- b) Selection of tools, libraries, languages:
 - 1) Tools shall be suitable for the application. Technical features which detect conditions that can cause systematic error (such as data type mismatch, ambiguous dynamic memory allocation, incomplete called interfaces, recursion, pointer arithmetic) shall be used. Checks shall mainly be carried out during compile time and not only at runtime. Tools should enforce language subsets and coding guidelines or at least supervise or guide the developer using them. For PL e achieved with one component and its tool, the tool shall be in conformity with the applicable component standard. If two diverse components with diverse tools are used, successful operating experience gained from prior projects can be sufficient.
 - 2) Whenever reasonable and practicable, validated function block libraries should be used – either safety-related function block libraries provided by the tool manufacturer (highly recommended for PL e) or validated application specific FB libraries and in conformity with this document.
 - 3) A justified LVL-subset suitable for a modular approach should be used (see [7.2.1](#)), e.g. accepted subset of IEC 61131-3 languages.
- c) Software design shall feature:
 - 1) semi-formal methods to describe data and control flow, e.g. state diagram or program flow chart;
 - 2) modular and structured programming predominantly realized by function blocks deriving from safety-related validated function block libraries or other modularity structure to achieve easy code reading and testability;
 - 3) function blocks of limited size of coding;
 - 4) code execution inside function block with only one entry and only one exit point;
 - 5) architecture model of three stages: inputs $\Rightarrow$ processing $\Rightarrow$ outputs (see [Figure 16](#) and [Annex J](#));
 - 6) assignment of a safety output at only one program location;
 - 7) use of techniques for detection and control of hardware failure and for defensive programming within input, processing and output blocks which lead to safe state.

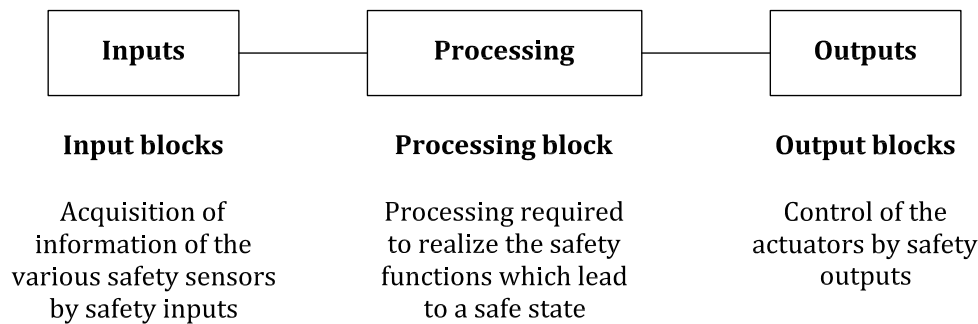


Figure 16 — General architecture model of software

- d) Where SRASW and non-SRASW are combined in one component:
- 1) SRASW and non-SRASW shall be coded in different function blocks with well-defined interfaces;
 - 2) there shall be no logical combination of non-safety-related and safety-related data which can lead to downgrading of the integrity of safety-related signals, for example, combining safety-related and non-safety-related signals by a logical "OR" where the result controls safety-related signals.
- e) Software implementation/coding:
- 1) code shall be readable, understandable and testable and, because of this, symbolic variables (instead of explicit hardware addresses) should be used;
 - 2) justified or accepted coding guidelines shall be used (see also [Annex J](#));
 - 3) data integrity and plausibility checks (e.g. range checks) available on application layer (defensive programming) should be used;
 - 4) code should be tested by simulation;
 - 5) verification should be performed by control flow analysis and data flow analysis for PL d or e.
- f) Testing:
- 1) the appropriate validation method is black-box testing of functional behaviour and performance criteria (e.g. timing performance);
 - 2) for PL d or e, test case execution from boundary value analysis is recommended;
 - 3) test planning should include test cases with completion criteria and required tools;
 - 4) I/O testing shall ensure that safety-related signals are correctly used within SRASW.
- g) Documentation:
- 1) all lifecycle and modification activities shall be documented;
 - 2) documentation shall be complete, available, readable and understandable;
 - 3) code documentation within source text shall contain module headers with legal entity, functional and I/O description, version of used library function blocks, and sufficient comments of networks/statement and declaration lines.
- h) Verification:
- 1) Verification shall be performed by, e.g. review, inspection, walkthrough or other appropriate activities.

NOTE Verification is only used for application-specific code, and not for validated library functions.

i) Configuration management:

- 1) It is highly recommended that procedures and data backup be established to identify and archive documents, software modules, verification/validation results and tool configuration related to a specific SRASW version.

j) Modifications:

- 1) Prior to a modification of SRASW, an impact analysis shall be performed to ensure consistency with the software design. Appropriate lifecycle activities shall be performed after modifications. Means shall be provided to protect against unauthorized modifications to SRASW and the modification history shall be documented.

8 Verification of the achieved performance level

For each individual safety function, the PL of the related SRP/CS shall match or be greater than the required performance level (PL_r) determined according to 5.3 and 6.1.1. If this is not the case, iteration in the process described in Figure 4 is necessary.

The PL of the different subsystems which are part of a safety function shall be greater than or equal to the PL_r of this safety function (see 5.3 and 6.1.1).

9 Ergonomic aspects of design

The interface between operators and the SRP/CS shall be designed and realized to minimize exposures to hazards during the intended use and the reasonably foreseeable misuse of the machine due to neglecting ergonomic principles.

The ergonomic principles given in ISO 12100:2010, 6.2.8, apply.

NOTE Ergonomic principles are intended to improve the ease of use of the control systems to avoid motivation for defeating or unintended misuse of the machine. See ISO/TR 22100-3 and ISO 9241-210 for guidance on ergonomics.

10 Validation

10.1 Validation principles

10.1.1 General

The purpose of the validation process is to confirm that the SRP/CS meets the overall SRS created in accordance with Clause 5 and Clause 7.

Figure 17 gives an overview of the validation process. The validation consists of applying analysis (see 10.3) and executing tests (see 10.4) under foreseeable conditions in accordance with the validation plan.

NOTE 1 The SRP/CS validation ensures that the safety functions achieve the intended risk reduction and is intended to be part of the overall validation process of the machine.

The validation activities shall ensure the completeness and correctness of each design activity identified in the validation plan.

The validation to be applied to the SRP/CS includes inspection (e.g. by analysis) and testing of the SRP/CS to ensure that it achieves the requirements stated in the SRS (according to Clause 5).

The validation shall demonstrate that the SRP/CS meets the requirements and, in particular, the following:

- a) the specified functional requirements of the safety functions provided by that part, as set out in the SRS;
- b) the requirements of the specified PL in accordance with [6.1.1](#):
 - 1) the requirements of the specified category,
 - 2) the measures for control and avoidance of systematic failures (systematic integrity),
 - 3) if applicable, the requirements of the software, and
 - 4) the ability to perform a safety function under expected environmental conditions;
- c) the ergonomic design, interaction and positioning of the operator interface.

The validation process should be carried out by person(s) who is/are independent from the design of the SRP/CS.

NOTE 2 An independent person is a person not involved in the design of the SRP/CS and does not necessarily mean that a third-party is required.

The analysis should be started as early as possible, and in parallel with, the design process. It can be necessary for some parts of the analysis to be delayed until the design is well developed.

NOTE 3 Problems can then be corrected early while they are still relatively easy to correct, i.e. during steps “design and technical realization of the safety function” and “evaluate the PL”.

Where necessary due to the size of the system, complexity or the effects of integrating it with the control system (of the machinery), special arrangements should be made for

- validation of the subsystem separately before integration, including simulation of the appropriate input and output signals, and
- validation of the effects of integrating SRP/CS into the remainder of the control system within the context of its use in the machine.

The balance of analysis and testing depends on the technology used for the SRP/CS and the required performance level (PL_r). For categories 2, 3 and 4 the validation of the safety function shall also include testing by appropriate fault injection to show that among other things, the fault reaction will be initiated by the implemented diagnostic function.

“Modification of the design” in [Figure 17](#) refers to the design process. If the validation cannot be successfully completed, changes in the design are necessary. The validation of the modified parts of the SRP/CS shall then be repeated. This process shall be iterated until the SRP/CS for each safety function is successfully validated.

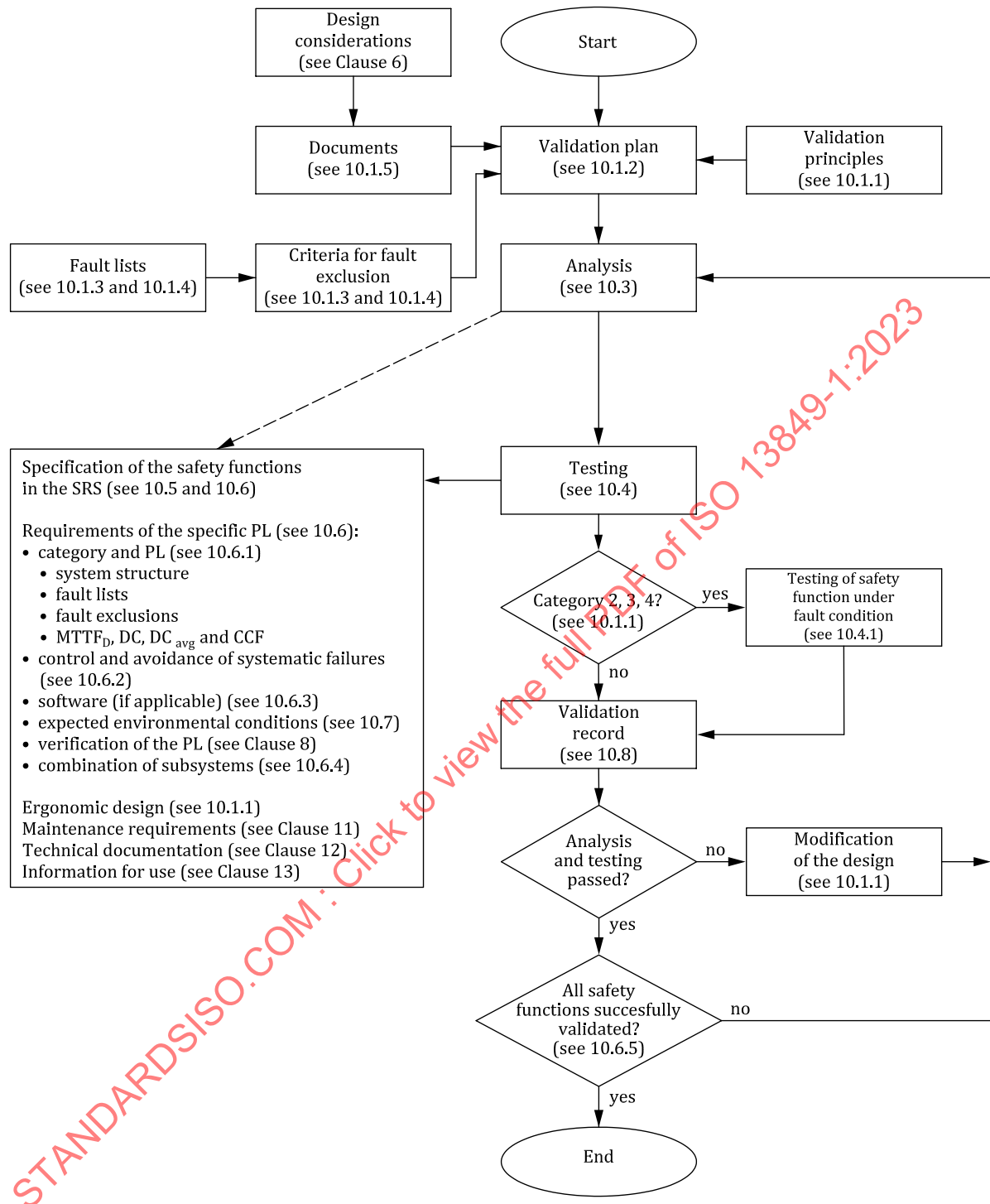


Figure 17 — Overview of the validation process

10.1.2 Validation plan

The validation plan shall identify and describe the requirements for carrying out the validation process and shall be made available to affected persons and parties involved in the validation process. The validation plan shall also identify the means to be employed to validate the specified safety functions. It shall identify, where appropriate

- the specification documents,
- the operational and environmental conditions during testing,

- c) the analyses and tests to be applied,
- d) the reference to test standards to be applied, and
- e) the persons or parties responsible for each step in the validation process.

10.1.3 Generic fault lists

Validation involves consideration of the behaviour of the SRP/CS for all faults to be considered. A basis for fault consideration is given in the tables of fault lists in ISO 13849-2:2012, Annexes A to D, which are based on experience and which contain

- the components/elements to be included, e.g. conductors/cables,
- the faults to be taken into account, e.g. short circuits between conductors,
- the permitted fault exclusions, taking into account environmental, operating and application aspects, and
- a remarks section giving the reasons for the fault exclusions.

Only permanent faults are taken into account in the fault lists.

10.1.4 Specific fault lists

If necessary, a specific product-related fault list shall be generated as a reference document for the validation of the subsystem(s) and/or subsystem element(s). The list can be based on the appropriate generic list(s) found in the annexes of ISO 13849-2:2012 or (reoccurring) faults found as a result of product observation.

Where the specific product-related fault list is based on the generic list(s) it shall state

- a) the faults taken from the generic list(s) to be included,
- b) any other relevant faults to be included but not given in the generic list (e.g. common-cause failures),
- c) the faults taken from the generic list(s) which may be excluded on the basis that the criteria given in the generic list(s) are satisfied, and
- d) in exceptional circumstances, any other faults for which justification and rationale for an exclusion is presented.

Where this list is not based on the generic list(s), the designer shall give the rationale for fault exclusions.

10.1.5 Information for validation

The information required for validation varies with the technology used, the category or categories and PL to be demonstrated, SRS, and the contribution of the SRP/CS to the reduction of the risk. Documents containing sufficient information from the following list shall be included in the validation to demonstrate that the SRP/CS perform the specified safety functions to the required PL and category:

- a) SRS, including the required characteristics of each safety function, e.g. response time (according to ISO 13855:2010), operating mode, PL, interfaces between the subsystems of the SRP/CS and if necessary characteristics of used category of each subsystem of the SRP/CS;
- b) drawings and specifications, e.g. for mechanical, hydraulic and pneumatic parts, printed circuit boards, assembled boards, internal wiring, enclosure, materials, mounting;
- c) block diagram(s) and where needed for clarification with a functional description of the blocks;
- d) circuit diagram(s), including interfaces/connections;

- e) functional description of the circuit diagram(s), where needed for clarification;
- f) time sequence diagram(s) for switching components, signals relevant for safety;
- g) description of the relevant characteristics of components previously validated;
- h) for SRP/CS other than those listed in g), component lists, e.g. with item designations, rated values, tolerances, relevant operating stresses, type designation, failure rate data and component manufacturer, and any other data relevant to safety;

NOTE 1 Data can be provided in libraries according to VDMA 66413.

- i) report of analysis of all relevant faults according to [10.1.3](#) and [10.1.4](#), such as those listed in the tables of ISO 13849-2:2012, Annexes A to D, including the justification of any excluded faults;
- j) report of analysis of the influence of processed materials;
- k) information for use, maintenance requirements, e.g. installation and operation manual/instruction handbook.

Where software is relevant to the safety function(s), the software documentation shall include

- a specification which is clear and unambiguous,
- evidence that the software is designed to achieve the required PL (see [10.6.3](#)), and
- details of tests (in particular test reports) carried out to prove that the required PL is achieved.

Information is required on how the PL and PFH is determined. The documentation of the quantifiable aspects shall include

- the safety-related block diagram or designated architecture according to [6.1.3.2](#),
- the determination of $MTTF_D$, DC_{avg} and CCF, and
- the determination of the category.

NOTE 2 For guidance on safety-related block diagram see [Annex B](#).

Information is required for documentation on measures against systematic failures of the SRP/CS.

Information is required to describe how the combination of several subsystems achieves the required PL.

NOTE 3 Where practicable, a clear and traceable reference to existing documents is acceptable.

10.2 Validation of the safety requirements specification (SRS)

Prior to the validation of the design of the SRP/CS or the combination of subsystems providing the safety function, the requirements specification for the safety function shall be verified to ensure consistency and completeness for its intended use (see [5.4](#)).

In order to validate the specification, appropriate measures to detect systematic failures (errors, omissions or inconsistencies) shall be applied.

Validation can be performed by reviews and inspections of the SRS, in particular considering

- the intended application requirements,
- the risk assessment,
- the operational and environmental conditions, and
- reasonably foreseeable misuse.

10.3 Validation by analysis

10.3.1 General

Validation of the SRP/CS shall be carried out by analysis. Inputs to the analysis include the following:

- the safety function(s), their characteristics and the safety integrity specified according to 5.2;
- the system structure (e.g. designated architectures) according to 6.1.3.2;
- the quantifiable aspects ($MTTF_D$, DC_{avg} and CCF) according to 6.1.4, 6.1.5, and 6.1.6 by validating assumptions and data that were associated in selecting the values used in the system calculations;
- the non-quantifiable, qualitative aspects which affect system behaviour (if applicable, software aspects);
- deterministic arguments;
- fault lists;
- criteria for fault exclusion.

NOTE A deterministic argument is an argument based on qualitative aspects (e.g. quality of manufacture, experience of use). This consideration depends on the application, which, together with other factors, can affect the deterministic arguments. Deterministic arguments differ from other evidence in that they show that the required properties of the system follow logically from a model of the system. Such arguments can be constructed on the basis of simple, well-understood concepts.

10.3.2 Analysis techniques

The following are two basic techniques that can be used for analysis:

- a) Top-down (deductive) techniques are suitable for determining the initiating events that can lead to identified top events and calculating the probability of top events from the probability of the initiating events. They can also be used to investigate the consequences of identified multiple faults.

EXAMPLE 1 FTA (see IEC 61025), ETA (see IEC 62502).

- b) Bottom-up (inductive) techniques are suitable for investigating the consequence of identified single faults.

EXAMPLE 2 FMEA (see IEC 60812) and failure modes, effects and criticality analysis (FMECA) (see IEC 60812).

10.4 Validation by testing

10.4.1 General

Testing shall be part of the validation. In case the category is B or 1, tests under fault conditions are not required and analysis with functional testing may be sufficient.

Validation tests shall be planned and implemented in a logical manner. In particular:

- a) a test plan shall be produced before testing begins that shall include
 - 1) the test specifications,
 - 2) the required outcome of the tests for conformity, and

- 3) the chronology of the tests, if applicable;
- b) test records shall be produced that include:
 - 1) the name of the person carrying out the test,
 - 2) the environmental conditions,
 - 3) the test procedures and equipment used,
 - 4) the date of the test, and
 - 5) the results of the test;
- c) the test records shall be compared with the test plan to ensure that the specified functional and performance targets are achieved.

The test sample shall be operated as near as possible to its final operating configuration, i.e. with all peripheral devices and covers attached.

This testing may be applied manually or automatically, e.g. by computer.

Where applied, validation of the safety functions by testing shall be carried out by applying input signals, in various combinations, to the SRP/CS. The final response at the outputs shall be compared to the appropriate specified outputs.

The combination of these input signals should be applied systematically to the control system and the machine, e.g. power-on, start-up, operation, directional changes and restart-up. An expanded range of input data should be applied to take into account anomalous or unusual situations, in order to see how the SRP/CS responds. Such combinations of input data should take into account foreseeable incorrect operation(s).

When validation by analysis is not conclusive, testing shall be carried out to complete the validation. Testing is always complementary to analysis and is often necessary.

10.4.2 Measurement accuracy

The accuracy of measurements during the validation by testing shall be appropriate for the test carried out. In general, these measurement accuracies shall be within ± 5 K for temperature measurements and ± 5 % for the following:

- a) time measurements;
- b) pressure measurements;
- c) force measurements;
- d) electrical measurements;
- e) relative humidity measurements;
- f) linear measurements.

Deviations from these measurement accuracies shall be justified.

10.4.3 Additional requirements for testing

If the SRP/CS is required to fulfil more stringent requirements than those within this document, the testing shall be extended to cover these more stringent requirements as well.

NOTE Depending on the risk assessment, more stringent requirements can apply if the control system has to withstand particularly adverse service conditions, e.g. rough handling, humidity effects, hydroxylation, ambient temperature variations, effects of chemical agents, corrosion, and high strength of electromagnetic fields, for example, due to close proximity of transmitters.

10.4.4 Number of test samples

Unless otherwise specified in the test specification, the tests shall be made on a single production sample of the subsystem being tested.

Subsystem(s) under test shall not be modified during the course of the tests.

Certain tests can permanently change the performance of some components. Where a permanent change in a component causes the safety-related part to be incapable of meeting the requirements of further tests, a new sample or samples shall be used for subsequent tests.

Where a particular test is destructive and equivalent results can be obtained by testing part of SRP/CS in isolation, a sample of that part of the SRP/CS may be used instead of the whole SRP/CS for the purpose of obtaining the results of the test. This approach shall only be applied where it has been shown by analysis that testing of a part of SRP/CS is sufficient to demonstrate the safety integrity of the whole SRP/CS that performs the safety function.

10.4.5 Testing methods

Depending on the application, different testing methods shall be used to validate the SRP/CS. In some applications it can be necessary to divide the connected SRP/CS into several functional groups and to subject these groups and their interfaces to fault simulation tests. The precise instant at which a fault is injected into a system can be critical. The worst-case effect of a fault injection shall be determined by analysis and by injecting the fault at this appropriate critical time. Common test methods are:

- a) simulation of control system behaviour in the event of a fault, e.g. by means of either hardware or software models, or both;
- b) software simulation of faults;
- c) functional testing of the safety functions in all operating modes of the machine, to establish whether they meet the specified characteristics (see [Clause 5](#)). The functional tests shall ensure that all safety-related outputs are realized over their complete ranges and respond to safety-related input signals in accordance with the specification. The test cases are normally derived from the specifications but can also include some cases derived from analysis of the schematics or software;
- d) extended functional testing to check foreseeable abnormal signals or combinations of signals from any input source, including power interruption and restoration, and incorrect operations;
- e) fault injection tests on the actual circuit and fault initiation on actual components, particularly in parts of the system where there is doubt regarding the results obtained from failure analysis;
- f) fault injection tests into a production sample;
- g) fault injection tests into a hardware model;
- h) subsystem failure test (e.g. power supplies).

10.5 Validation of the safety functions

The validation of safety functions shall demonstrate that the SRP/CS, or combination of subsystems, provides the safety function(s) in accordance with their specified characteristics.

Validation of the specified characteristics of the safety functions shall be achieved by the application of appropriate measures from the following list:

- a) Functional analysis of schematics, reviews of the software (see [10.6.3](#)).

NOTE Where a machine has complex or a large number of safety functions, an analysis can reduce the number of functional tests required.

- b) Simulation.
- c) Check of the hardware components installed in the machine and details of the associated software to confirm their correspondence with the documentation (e.g. manufacturer, type, version).
- d) Functional testing (see [10.4.5](#)).
- e) Check of the operator-SRP/CS interface for the meeting of ergonomic principles.

10.6 Validation of the safety integrity of the SRP/CS

10.6.1 Validation of subsystem(s)

The safety integrity of each subsystem of the SRP/CS shall be validated by confirming the requirements of [Table 10](#) according to the category used.

Table 10 — Basic requirements for categories to be validated

Requirements	Category				
	B	1	2	3	4
Basic safety principles	X	X	X	X	X
Expected operating stresses	X	X	X	X	X
Influences of processed material	X	X	X	X	X
Performance during other relevant external influences	X	X	X	X	X
Well-trying components	—	X	—	—	—
Well-trying components for the case of determination the PL without $MTTF_D$	—	X	X	X	X
Well-trying safety principles	—	X	X	X	X
$MTTF_D$ of each channel	X	X	X	X	X
The recognizable faults and the associated diagnostic measures, including fault reaction	—	—	X	X	X
Checking intervals, when specified	—	—	X	X	X
DC_{avg}	—	—	X	X	X
CCF identified and how to prevent them	—	—	X	X	X
Justification for fault exclusion	X	X	X	X	X
How the safety function is maintained in the case of each of the faults	—	—	—	X	X
How the safety function is maintained for each of the combinations of faults	—	—	—	—	X
Measures against systematic failures	X	X	X	X	X
Key X required — not required NOTE The categories are those given in 6.1.3.2 .					

Table 10 (continued)

Requirements	Category				
	B	1	2	3	4
Measures against software faults	X	—	X	X	X
Key X required — not required NOTE The categories are those given in 6.1.3.2.					

In addition, the safety integrity of each subsystem of the SRP/CS shall be validated by confirming

- the probability of dangerous random hardware failure, and
- the systematic integrity (see [Annex G](#), [Clause 7](#) Software, CCF).

In this context the validation of $MTTF_D$ (including B_{10D} , T_{10D} and n_{op} values), DC_{avg} and CCF is typically performed by analysis and visual inspection.

Where fault exclusion claims mean that particular components do not contribute to the channel $MTTF_D$, the plausibility of the fault exclusion shall be checked.

NOTE A fault exclusion implies infinite $MTTF_D$, therefore, fault excluded failure modes of the component do not contribute to the calculation of channel $MTTF_D$.

The $MTTF_D$ of each channel of the subsystem, including application of the symmetrisation formula (see [Annex D](#)) to dissimilar redundant channels, shall be checked for correct calculation. $MTTF_D$ of individual channels shall be restricted to no greater than 100 years (2 500 years for category 4) before the symmetrisation formula is applied.

The DC values for either components (subsystem elements) or logic blocks, or both, shall be checked for plausibility (e.g. against measures in [Annex E](#)). The correct implementation (hardware and software) of checks and diagnostics, including appropriate fault reaction, shall be validated by testing under typical environmental conditions in use.

The correct implementation of sufficient measures against common-cause failures shall be validated (e.g. [Annex F](#)). Typical validation measures are static hardware analysis and functional testing under environmental conditions.

Generally, for the specification of the $MTTF_D$ values of electronic components, an ambient temperature of +40 °C is taken as a basis. During validation, it is important to ensure that, for $MTTF_D$ values, the environmental and functional conditions (in particular temperature) taken as basis are met. Where a device, or component, is operated significantly above (e.g. > 10 °K) the specified temperature of +40 °C, it is necessary to use $MTTF_D$ values for the increased ambient temperature.

10.6.2 Validation of measures against systematic failures

The validation of measures against systematic failures can typically be provided by:

- a) inspections of design documents which confirm the application of
 - 1) basic and well-tried safety principles (see ISO 13849-2:2012, Annexes A to D),
 - 2) further measures for avoidance of systematic failures according to [Annex G](#), and
 - 3) further measures for the control of systematic failures, such as hardware diversity, modification protection or failure assertion programming;
- b) failure analysis (e.g. FMEA);
- c) fault injection tests/fault initiation;

- d) inspection and testing of data communication, where used;
- e) checking that a quality management system is used to avoid systematic failures in the manufacturing process.

NOTE Systematic faults can be caused by errors made during the design and integration stages (e.g. a misinterpretation of the safety function characteristics, an error in the logic design, an error in hardware assembly, an error in typing the code of software). Some of these errors will be revealed during the design process, while others will be revealed during the validation process or will remain unnoticed. In addition, it is possible for an error to be made (e.g. failure to check a characteristic) during the validation process.

10.6.3 Validation of safety-related software

The validation of software shall include

- the specified functional behaviour and performance criteria (e.g. timing performance) of the software when performed on the target hardware,
- verification that the software measures are sufficient for the specified PL_r of the safety function, and
- verification that the protective measures and activities planned to be taken during software development to avoid systematic software faults have been employed, by inspecting the documented evidence.

As a first step, check that there is documentation for the specification and design of the safety-related software. This documentation shall be reviewed for completeness and absence of erroneous interpretations, omissions or inconsistencies.

In general, software can be considered a “black box” or “grey box” (see [Clause 7](#)) and validated by the black- or grey-box test, respectively.

NOTE 1 In the case of small programs, an analysis of the program by means of reviews or walk-through of control flow, procedures, using the software documentation (control flow chart, source code of modules or blocks, I/O and variable allocation lists, cross-reference lists) can be sufficient.

NOTE 2 Black-box testing aims to check the dynamic behaviour under real functional conditions, and to reveal failures to meet functional specification, and to assess utility and robustness. Grey-box testing is similar to black-box testing but additionally monitors relevant test parameter(s) inside the software module.

Depending on the PL_r , the tests should include

- black-box or grey-box testing of functional behaviour and performance (e.g. timing performance),
- additional extended test cases based upon limit value analyses, recommended for PL_d or PL_e ,
- I/O tests to ensure that the safety-related input and output signals are used properly, and
- test cases which simulate faults determined analytically beforehand, together with the expected response, in order to evaluate the adequacy of the software based measures for control of failures.

NOTE 3 See [N.2](#) for an example.

Individual software functions which have already been validated do not need to be validated again. Where a number of such safety function blocks are combined for a specific project, however, the resulting total safety function shall be validated.

The measures for software implementation and configuration and modification management according to [Clause 7](#), which depend on the PL to be attained, shall be examined with regard to their proper implementation.

Should the safety-related software be subsequently modified, it shall be revalidated on an appropriate scale.

10.6.4 Validation of combination of subsystems

Where the safety function is implemented by two or more subsystems, validation of the combination – by analysis and by testing – shall be undertaken to establish that the combination achieves the safety integrity specified in the design. Existing recorded validation results of subsystems can be taken into account. The following validation steps shall be performed:

- inspection of design documents describing the overall safety function(s);
- a check that the overall PL of the subsystem combination has been correctly evaluated, based on the PL of each individual subsystem (according to 6.2);
- consideration of the characteristics of the interfaces, e.g. voltage, current, pressure, data format of information, signal level;
- failure analysis relating to combination/integration, e.g. by FMEA;
- testing of the subsystem combination;
- for redundant systems, fault injection tests relating to combination/integration.

10.6.5 Overall validation of safety integrity

The following steps shall be performed:

- checking/verification for correct evaluation of PL, based on PFH and PL/SIL of subsystems (see 7.2);
- checking/verification for correct evaluation of PL based on the category, DC_{avg} and $MTTF_D$, CCF and measures against systematic failures;
- checking/verification that the PL achieved by the SRP/CS satisfies the PL_r in the SRS for the machinery: $PL \geq PL_r$.

10.7 Validation of environmental requirements

The performance specified in the design of the SRP/CS shall be validated with respect to the environmental conditions specified for the control system.

Validation shall be carried out by analysis and by testing. The extent of the analysis and of the testing depends upon the safety-related parts, the system in which they are installed, the technology used, and the environmental condition(s) being validated. The use of operational reliability data on the system or its components, or the confirmation of conformity to appropriate environmental standards (e.g. for waterproofing, vibration protection) can assist this validation process.

Where applicable, validation shall address

- expected mechanical stresses from shock, vibration, ingress of contaminants,
- mechanical durability,
- electrical ratings and power supplies,
- climatic conditions (temperature and humidity), and
- EMI (immunity).

When testing is needed to determine conformity with the environmental requirements, the procedures outlined in the relevant standards shall be followed as far as required for the application.

After the completion of validation by testing, the safety functions shall continue to be in accordance with the specifications for the safety requirements, or the SRP/CS shall provide output(s) for a safe state.

10.8 Validation record

Validation by analysis and testing shall be recorded. The record shall demonstrate the validation process for each of the safety requirements. Cross-reference may be made to previous validation records, provided they are properly identified.

For any safety-related part which has failed an element of the validation process, the validation record shall describe which elements in the validation analysis/testing have failed. It shall be ensured that all SRP/CS are successfully re-validated after modification.

10.9 Validation maintenance requirements

The validation process shall demonstrate that the provisions for maintenance requirements have been implemented.

Validation of maintenance requirements shall include the following, as applicable:

- a) a review of the information for use confirming that
 - 1) maintenance instructions are complete [including procedures, required tools, frequency of inspections, time interval for changing components subjected to wear (T_{10D}) etc.] and understandable,
 - 2) if appropriate, there are provisions for the maintenance to be performed only by skilled maintenance personnel;
- b) a check that measures for ease of maintainability (e.g. provision of diagnostic tools to aid fault-finding and repair) have been applied.

In addition, the following measures shall be included when applied:

- measures against mistakes during maintenance (e.g. detection of wrong input data via plausibility checks);
- measures against modification (e.g. password protection to prevent access to the program by unauthorized persons).

11 Maintainability of SRP/CS

Preventive or corrective maintenance can be necessary to maintain the specified performance of the SRP/CS.

NOTE Exceeding specified lifetime or test interval can lead to deterioration in safety or to a hazardous situation.

The following factors shall be taken into account to enable maintenance of the SRP/CS:

- accessibility, taking into account the environment and the human body measurements, including the dimensions of the working clothes and tools used;
- ease of handling, taking into account ergonomic capabilities;
- limitation of the number of special tools and equipment where possible;
- indication(s) that maintenance is necessary (e.g. increased vibration) ideally with automated generation of warning signals (e.g. lifetime recording, self-test, monitoring of process parameters);
- required illumination levels.

12 Technical documentation

When designing an SRP/CS according to this document at least the following information relevant to the safety-related part shall be documented for internal purposes:

- a) SRS (see [5.2.1](#));
- b) exact points at which the safety-related part(s) starts and ends;
- c) decomposition into subsystems (see [5.2.2](#)), if applicable;
- d) environmental conditions (e.g. EMI immunity, temperature, vibration);
- e) achieved performance level and PFH value;
- f) category or categories selected (may not be applicable for previously validated subsystems);
- g) parameters relevant to the reliability ($MTTF_D$, DC, CCF and T_{10D}) and the mission time;
- h) measures against systematic failure;
- i) the technology or technologies used;
- j) the safety-relevant faults considered;
- k) justification for fault exclusions (see [6.1.10.3](#) and all annexes of ISO 13849-2:2012);
- l) software documentation if applicable;
- m) measures against reasonably foreseeable misuse;
- n) safety-related block diagram;
- o) relevant design documentation, test, verification and validation records, where applicable.

NOTE The design documentation is generally foreseen to be used for internal purposes of the manufacturer or to exchange technical information between sub-contractors (e.g. external system designer, certification body) and the manufacturer. The design documentation is also necessary to fulfil legal documentation requirements. The design documentation does not need to be distributed to the machine user but parts of it are relevant to prepare adequate information for use (see [Clause 13](#)).

13 Information for use

13.1 General

The information for use of the SRP/CS shall be according to ISO 20607:2019 or IEC/IEEE 82079-1:2019 including the relevant instructions for the intended target groups. The lifecycle phases of the machine where an SRP/CS is involved shall be covered by this information.

13.2 Information for SRP/CS integration

The information which is important for the correct integration of SRP/CS shall be given to the integrator. This shall include, but is not limited to the following:

- a) the limits of the safety-related parts of an SRP/CS selected (e.g. environmental conditions, such as EMI immunity, temperature, vibration) and appropriate information to ensure the continued justification of the fault exclusions, e.g. regarding modification, maintenance and repair;
- b) clear descriptions of the interfaces to the SRP/CS and protective devices;
- c) response time where relevant (according to ISO 13855:2010);

- d) operating limits (e.g. demand frequency);
- e) indications and alarms;
- f) muting and suspension of safety functions;
- g) control modes and reset;
- h) maintenance (see [Clause 11](#));
- i) maintenance check lists;
- j) how to access and replace the parts of SRP/CS;
- k) means for easy and safe trouble shooting;
- l) test intervals where relevant;
- m) mission time.

NOTE The integrator can be a manufacturer, assembler, engineering company or the user.

Specific information for each safety function on categories and performance level shall be provided (see [5.3](#)), as follows:

- the categories of the subsystems forming the SRP/CS (may not be applicable for previously validated subsystems);
- the performance level, a, b, c, d or e;
- the PFH value for SRP/CS related to the safety function, if relevant per subsystem(s).

13.3 Information for user

The information which is important for the correct use of SRP/CS shall be provided to the machine user (e.g. operator).

This can include, but is not limited to, the relevant aspects of [13.1](#) and [13.2](#). Relevant information with respect to testing of the safety functions shall also be provided. The designer of the SRP/CS shall provide information for use that describes the necessary maintenance tasks for the SRP/CS.

Information for maintenance can include tasks and applications, for example:

- a) setting;
- b) teaching/programming;
- c) process /tool changeover;
- d) cleaning;
- e) preventive maintenance;
- f) corrective maintenance;
- g) troubleshooting/fault finding;
- h) nature and frequency of inspections of safety functions;
- i) instructions relating to maintenance operations which require either technical knowledge or particular skills, or both, and hence should be carried out exclusively by qualified personnel (e.g. maintenance staff, specialists);

- j) instructions relating to maintenance actions (e.g. replacement of parts) which do not require specific skills and hence may be carried out by machine users (e.g. operators). It should be brought to the attention of maintenance staff which parts are critical to safety and shall only be replaced with original parts or parts fulfilling the same safety requirements;
- k) controlling hazardous energy (manual measures/other means) guidance, signs, and devices;
- l) drawings/diagrams enabling maintenance personnel to perform their tasks (especially fault-finding tasks to isolate conditions that caused the fault);
- m) information about replacement of components at or before the T_m period ends (for pneumatic, mechanical and electromechanical components see also [C.4.2](#)).

NOTE 1 For additional information see ISO 20607:2019 and IEC 60204-1:2016+AMD1:2021, 17.2 f.

If any maintenance activity requires the repair or modification of an SRP/CS revalidation including functional test shall be performed.

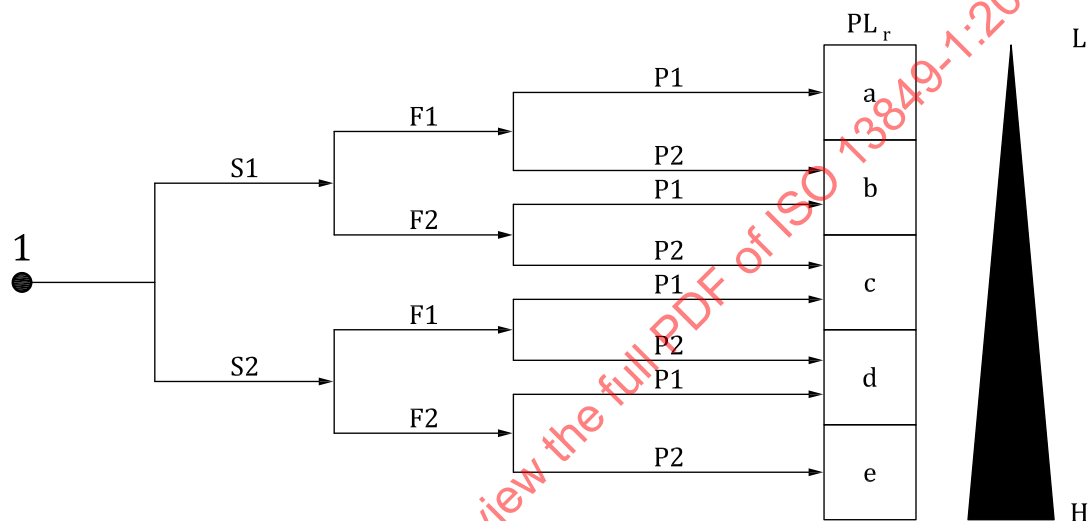
NOTE 2 The relevant revalidation activities would be dependent upon the extent of differences between the original and the replacing component.

STANDARDSISO.COM : Click to view the full PDF of ISO 13849-1:2023

Annex A
(informative)

Guidance for the determination of required performance level
(PL_r)

A.1 General



Key

- 1 starting point for evaluation of safety function's contribution to risk reduction
- L low contribution to risk reduction
- H high contribution to risk reduction
- PL_r required performance level

Risk parameters:

- S severity of injury
- S1 slight (normally reversible injury)
- S2 serious (normally irreversible injury or death)
- F frequency and/or exposure times to hazard
- F1 seldom-to-less-often and/or exposure time is short
- F2 frequent-to-continuous and/or exposure time is long
- P possibility of avoiding or limiting harm
- P1 possible under specific conditions
- P2 scarcely possible

Figure A.1 — Diagram for determining PL_r for safety function

Figure A.1 provides guidance for the determination of the safety-related PL_r for the safety function. The diagram should be considered for each safety function.

A.2 Selection of required performance level (PL_r)

[Annex A](#) is concerned with the contribution to the risk reduction made by the SRP/CS being considered. The method given in this clause is based on the estimation of risk parameters (which is by nature partly subjective as for any other risk estimation method). Therefore, this method is only a guidance to machine designers and standard makers for estimating the PL_r for each safety function to be carried out by an SRP/CS.

This methodology to estimate the PL_r is not mandatory. It is a generic approach which assumes a worst-case probability of occurrence of a hazardous event (the probability of occurrence is 100 %). In cases where the probability of occurrence can be assessed as low (this decision should be justified and documented), a downgrade by one performance level is possible otherwise the probability of occurrence is 100 %. Other risk estimation methods for specific types of machines can be used as appropriate and experience in successfully dealing with similar machines/hazards should be taken into account when estimating PL_r. Therefore, the PL required by a type-C standard can deviate from that indicated by the generic approach given in [Figure A.1](#).

The diagram in [Figure A.1](#) is based on the situation prior to the provision of the intended safety function (see also ISO/TR 22100-2:2013). Risk reduction by technical measures independent of the control system (e.g. mechanical guards), or additional safety functions, are to be taken into account in determining the PL_r of the intended safety function, in which case, the starting point of [Figure A.1](#) is selected after the implementation of these measures (see also [Figure 3](#)).

The parameters used in determining the PL_r are:

- severity of injury (S);
- frequency and/or exposure times to hazard (F);
- possibility of avoiding or limiting harm (P).

These parameters can be combined, as in [Figure A.1](#), to give a gradation of the contribution to required risk reduction from low to high.

A.3 Guidance for selecting parameters S, F and P for the risk estimation

A.3.1 Severity of injury, S1 and S2

In estimating the risk, only slight injuries or serious injuries are considered.

To make a decision, the usual consequences of accidents and normal healing processes should be taken into account in determining S1 and S2. For example, bruising and/or lacerations without complications would be classified as S1, whereas amputation or death would be S2.

NOTE For guidance about the evaluation of severe or slight injury see also ISO/TR 14121-2.

A.3.2 Frequency and/or exposure times to hazard, F1 and F2

A generally valid time period to be selected for parameter F1 or F2 cannot be specified. However, the following explanation can facilitate the decision-making process.

F2 should be selected if a person is frequently or continuously exposed to the hazard. It is irrelevant whether the same or different persons are exposed to the hazard on successive exposures, e.g. for the use of lifts. The frequency parameter should be chosen according to the frequency and duration of access to the hazard.

Where the demand on the safety function is known by the designer, the frequency and duration of this demand can be chosen instead of the frequency and duration of access to the hazard. In this document, the frequency of demand on the safety function is assumed to be more than once per year.

The period of exposure to the hazard should be evaluated on the basis of an average value which can be seen in relation to the total period of time over which the equipment is used. For example, if it is necessary to reach regularly between the tools of the machine during cyclic operation in order to feed and move workpieces, then F2 should be selected.

In case of no other justification, F2 should be chosen if the frequency is higher than once per 15 min.

F1 may be chosen if the accumulated exposure time does not exceed 1/20 of the overall operating time and the frequency is not higher than once per 15 min.

EXAMPLE At a machine with an overall operating time of 8 h per day a person is exposed 2 min once an hour to change workpieces (estimated average value) so the accumulated exposure time is 16 min in relation to 8 min × 60 min resulting in 1/30. Since also the frequency is 1/h, F1 can be chosen.

A.3.3 Possibility of avoiding or limiting harm, P1 and P2

It is important to know whether a hazardous event can be recognized before it can cause harm and be avoided. For example, can the exposure to a hazard be directly identified by its physical characteristics, or recognized only by technical means, e.g. indicators. Other important aspects which influence the selection of parameter P include, for example:

- a) speed with which the hazardous situation arises (e.g. quickly or slowly);
- b) possibilities to withdraw from the hazardous situation (e.g. avoidance by escaping);
- c) practical safety experiences relating to the process;
- d) whether operated by trained and suitable operators;
- e) operated with or without supervision.

When a hazardous event occurs, P1 should only be selected if there is a realistic possibility of avoiding or significantly reducing harm. Otherwise, P2 should be selected.

One possibility to determine P is the following approach:

- determine the letter of each factor of the [Table A.1](#) that reflects the specific application (only one choice for each factor is possible);
- count the number of chosen letters “A”, “B” and “C”;
- determine the corresponding value of the parameter P in [Table A.2](#).

Table A.1 — Determination of parameter P based on five factors

Factor	C	B	A
1. use of the machine by		unskilled person ^a	skilled person ^a
2. speed of the part of the machine that can create a hazardous event (depending on the specific machine and time to escape from or to avoid a hazardous situation)	high speed event e.g. > 1 000 mm/s, time to hazard <1 s and/or no or too little time to escape	medium speed event e.g. 251 mm/s to 1 000 mm/s, time to hazard ≥1 s and <3 s and/or limited time to escape	low or very low speed event e.g. < 250 mm/s, time to hazard ≥ 3 s and/or enough time to escape

NOTE Any numbers in this table are purely indicative and can be different in type-C standards or based on the specific machine application.

^a [3.1.55](#) defines a ‘skilled person’ which incorporates instruction and training as well as years of practice according to this document.

Table A.1 (continued)

Factor	C	B	A
3. spatial possibility to escape from the hazard	not possible	Occasionally/rarely possible possible in < 50 % of the cases	easily possible possible in ≥ 50 % of the cases
4. possibility of recognition/awareness of the hazard (e.g. hot/cold surface, non-ionising radiation etc.)	not possible e.g. instrumentation necessary, human senses are not able to perceive the hazard, environmental conditions hide the perception	occasional/rare recognition of the hazard possible in < 50 % of the cases	easy recognition of the hazard possible in ≥ 50 % of the cases
5. complexity of the operations (human interaction in terms of numbers of operation and/or timing available for this operations)		medium to high complexity e.g. troubleshooting, use hold-to-run control to setup a part of the machine	low complexity e.g. adjust the workpiece clamps, or very low complexity / or no interaction e.g. put a workpiece into the machine
NOTE Any numbers in this table are purely indicative and can be different in type-C standards or based on the specific machine application. a 3.1.55 defines a 'skilled person' which incorporates instruction and training as well as years of practice according to this document.			

Table A.2 — Selection of parameter P1 or P2

Overall score		Parameter "P"
one or more "C"	■ ■ ■ ■	P2
no "C", three or more "B"	■ ■ ■ ■	P2
no "C", two "B", the rest "A"	■ ■ ■ ■	P1 or P2 depending on the specific situation
no "C", one or no "B", the rest "A"	■ ■ ■ ■	P1

The approach based on [Table A.1](#) and [Table A.2](#) should always be used with the following basic intention: P1 should only be selected if there is a realistic possibility of avoiding harm or of significantly reducing its effect; otherwise P2 should be selected.

A.4 Overlapping hazards

When using this document, all hazards are considered as a specific hazard or hazardous situation. Each hazard can therefore be evaluated separately.

When it is obvious that there is a combination of directly linked hazards which always occur simultaneously then they should be combined during risk estimation.

The determination of whether hazards should be considered separately or in combination should be considered during the risk assessment of the machine.

EXAMPLE 1 A continuous welding robot can create various simultaneous hazardous situations, e.g. crushing caused by movement and burning due to the welding process. This can be considered as a combination of directly linked hazards.

EXAMPLE 2 For a robot cell in which separate robots are working, for the cell areas where only one robot can create at the same time a hazard, the robots can be considered separately.

EXAMPLE 3 As a result of a risk assessment it can be sufficient for a rotary table with clamping devices to consider each clamping device separately.

STANDARDSISO.COM : Click to view the full PDF of ISO 13849-1:2023

Annex B (informative)

Block method and safety-related block diagram

B.1 Block method

The simplified approach requires a block-oriented logical representation of the subsystem. The subsystem should be separated into a small number of blocks according to the following:

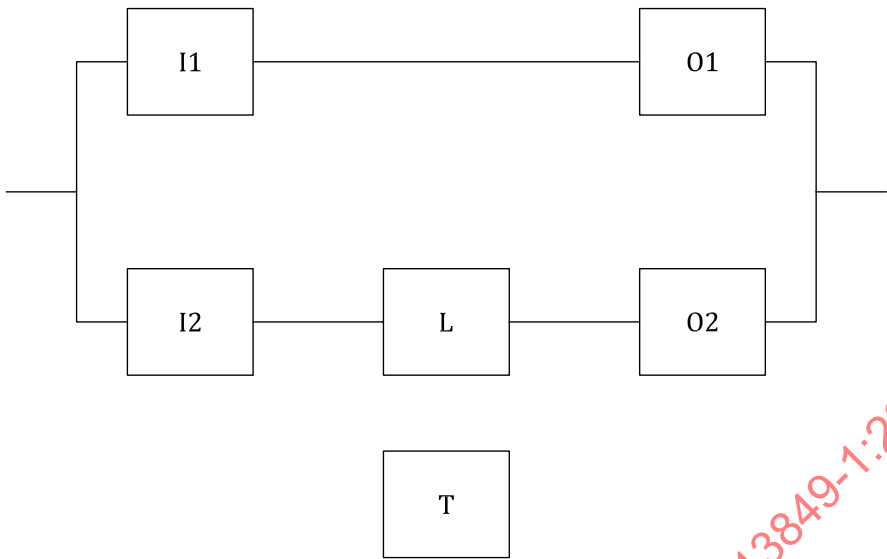
- a) blocks should represent logical units of the subsystem related to the execution of the safety function;
- b) different channels performing the sub-function should be separated into different blocks;
- c) if one block is no longer able to perform its function, the execution of the sub-function through the blocks of the other channel should not be affected;
- d) each channel may consist of one or several blocks – three blocks per channel in the designated architectures, input, logic and output, is not an obligatory number, but simply an example for a logical separation inside each channel;
- e) each hardware unit of the subsystem should belong only to one block, thus allowing for the calculation of the $MTTF_D$ of the block based on the $MTTF_D$ of the hardware units belonging to the block (e.g. by FMEA or the parts count method, see [D.1](#)).

B.2 Safety-related block diagram

The blocks defined by the block method may be used to graphically represent the logical structure of the subsystem in a safety-related block diagram. For such a graphical representation, the following guidance can be used:

- the failure of one block in a series alignment of blocks leads to the failure of the whole channel (e.g. if one hardware unit in one channel of the subsystem fails dangerously, the whole channel might not be able to execute the sub-function any longer);
- only the dangerous failure of all channels in a parallel alignment leads to the loss of the sub-function (e.g. a sub-function performed by several channels is performed as long as at least one channel has no failure); CCFs are capable of creating this type of condition (see [6.1.6](#) and [Annex F](#) and [Annex G](#));
- blocks used only for testing purposes of cat 3 or cat 4 SRP/CSs that do not affect the execution of the sub-function when they fail dangerously may be separated from blocks in the different channels.

See [Figure B.1](#) for an example.



Key	
I1, I2	input devices, e.g. sensor
L	logic
O1, O2	output devices, e.g. main contactor
T	testing device
I1 and O1	build up the first channel (series alignment)
I2, L and O2	build up the second channel (series alignment); with both channels executing the sub-function redundantly (parallel alignment)
T	used for testing only

Figure B.1 — Example of safety-related block diagram

Annex C (informative)

Calculating or evaluating $MTTF_D$ values for single components

C.1 General

This annex gives several methods for calculating or evaluating $MTTF_D$ values for single components: the method given in [C.2](#) is based on the application of good engineering practices for the different kinds of components; that given in [C.3](#) is applicable to hydraulic components; [C.4](#) provides a means of calculating the $MTTF_D$ of pneumatic, mechanical and electromechanical components from B_{10} (see [C.4.1](#)); [C.5](#) lists $MTTF_D$ values for electrical components.

C.2 Good engineering practices method

If the following criteria are met, the $MTTF_D$ or B_{10D} value for a component can be estimated according to [Table C.1](#).

- a) The components are manufactured according to basic and well-tried safety principles in accordance with ISO 13849-2:2012 and the relevant standard (see [Table C.1](#)) for the design of the component.

NOTE This information can be found in the data sheet of the component manufacturer.

- b) The manufacturer of the component specifies the appropriate application and operating conditions for the SRP/CS designer.
- c) The design of the SRP/CS fulfils the basic and well-tried safety principles according to ISO 13849-2:2012, for the implementation and operation of the component.

Table C.1 — International Standards dealing with $MTTF_D$ or B_{10D} for components

	Basic and well-tried safety principles according to ISO 13849-2:2012	Relevant standards	Typical values: $MTTF_D$ (years) B_{10D} (cycles)
mechanical components	Table A.1 and Table A.2	—	$MTTF_D = 150$
hydraulic components with $n_{op} \geq 1\,000\,000$ cycles per year ^a	Table C.1 and Table C.2	ISO 4413	$MTTF_D = 150$
hydraulic components with $1\,000\,000$ cycles per year $> n_{op} \geq 500\,000$ cycles per year ^a	Table C.1 and Table C.2	ISO 4413	$MTTF_D = 300$
hydraulic components with $500\,000$ cycles per year $> n_{op} \geq 250\,000$ cycles per year ^a	Table C.1 and Table C.2	ISO 4413	$MTTF_D = 600$
hydraulic components with $n_{op} < 250\,000$ cycles per year ^a	Table C.1 and Table C.2	ISO 4413	$MTTF_D = 1\,200$
pneumatic components	Table B.1 and Table B.2	ISO 4414	$B_{10D} = 20\,000\,000^c$
relays and contactor relays with small load	Table D.1 and Table D.2	IEC 61810-3 IEC 60947 series	$B_{10D} = 20\,000\,000$
relays and contactor relays with nominal load	Table D.1 and Table D.2	IEC 61810-3 IEC 60947 series	$B_{10D} = 400\,000$
proximity switches with small load	Table D.1 and Table D.2	IEC 60947 series ISO 14119	$B_{10D} = 20\,000\,000$
proximity switches with nominal load	Table D.1 and Table D.2	IEC 60947 series ISO 14119	$B_{10D} = 400\,000$
contactors with small load ^d	Table D.1 and Table D.2	IEC 60947 series	$B_{10D} = 20\,000\,000$
contactors with nominal load ^d	Table D.1 and Table D.2	IEC 60947 series	$B_{10D} = 1\,300\,000$
NOTE 1 For the definition and use of B_{10D}, see C.4. NOTE 2 B_{10D} is estimated as two times B_{10} (50 % dangerous failure) if no other information (e.g. product standard) is available. NOTE 3 Emergency stop devices according to IEC 60947-5-5 and ISO 13850 and enabling switches according to IEC 60947-5-8 can be estimated as a category 1 or category 3/4 subsystem depending on the number of electrical output contacts and on the fault detection in the subsequent subsystem. Each contact element (including the mechanical actuation) can be considered as one channel with a respective B_{10D} value. For enabling switches according to IEC 60947-5-8 this implies the opening function by pushing through or by releasing. In some cases, it is possible that the machine builder can apply fault exclusion according to ISO 13849-2:2012, Table D.8, considering the specific application and environmental conditions of the device. NOTE 4 Reduction of switching cycles can lead to an increasing probability of sticking of the switching elements in spool valves (see ISO 4413). NOTE 5 The $MTTF_D$ for mechanical components refers exclusively to mechanically moving components/parts (not to housing). ^a B_{10D} calculation for hydraulic components is not permitted as a reverse calculation from standard $MTTF_D$ values. ^b If fault exclusion for direct opening action is possible. ^c In general, this value can be assumed for most pneumatic components. However, depending on the application and type, e.g. shut-off valve, this value can be significantly lower. ^d "Nominal load" or "small load" should take into account safety principles described in ISO 13849-2:2012, such as over-dimensioning of the rated current value. "Small load" means, for example, 20 %.			

Table C.1 (continued)

	Basic and well-tried safety principles according to ISO 13849-2:2012	Relevant standards	Typical values: MTTF _D (years) B_{10D} (cycles)
position switches ^b	Table D.1 and Table D.2	IEC 60947 series ISO 14119	$B_{10D} = 20\,000\,000$
position switches (with separate actuator, guard-locking) ^b	Table D.1 and Table D.2	IEC 60947 series ISO 14119	$B_{10D} = 2\,000\,000$
emergency stop devices ^b	Table D.1 and Table D.2	IEC 60947 series ISO 13850	$B_{10D} = 100\,000$
push buttons (e.g. enabling switches) ^b	Table D.1 and Table D.2	IEC 60947 series	$B_{10D} = 100\,000$

NOTE 1 For the definition and use of B_{10D} , see C.4.

NOTE 2 B_{10D} is estimated as two times B_{10} (50 % dangerous failure) if no other information (e.g. product standard) is available.

NOTE 3 Emergency stop devices according to IEC 60947-5-5 and ISO 13850 and enabling switches according to IEC 60947-5-8 can be estimated as a category 1 or category 3/4 subsystem depending on the number of electrical output contacts and on the fault detection in the subsequent subsystem. Each contact element (including the mechanical actuation) can be considered as one channel with a respective B_{10D} value. For enabling switches according to IEC 60947-5-8 this implies the opening function by pushing through or by releasing. In some cases, it is possible that the machine builder can apply fault exclusion according to ISO 13849-2:2012, Table D.8, considering the specific application and environmental conditions of the device.

NOTE 4 Reduction of switching cycles can lead to an increasing probability of sticking of the switching elements in spool valves (see ISO 4413).

NOTE 5 The MTTF_D for mechanical components refers exclusively to mechanically moving components/parts (not to housing).

^a B_{10D} calculation for hydraulic components is not permitted as a reverse calculation from standard MTTF_D values.

^b If fault exclusion for direct opening action is possible.

^c In general, this value can be assumed for most pneumatic components. However, depending on the application and type, e.g. shut-off valve, this value can be significantly lower.

^d "Nominal load" or "small load" should take into account safety principles described in ISO 13849-2:2012, such as over-dimensioning of the rated current value. "Small load" means, for example, 20 %.

C.3 Hydraulic components

If the following criteria are met, the MTTF_D value for a single hydraulic component, e.g. valve, can be estimated at 150 years. If the mean number of annual operations (n_{op}) is below 1 000 000 cycles per year, then the MTTF_D value can be estimated higher as shown in Table C.1:

- The hydraulic components are manufactured according to basic and well-tried safety principles in accordance with ISO 13849-2:2012, Table C.1 and Table C.2 and the relevant standard (see Table C.1), for the design of the hydraulic component (confirmation in the data sheet of the component).
- The manufacturer of the hydraulic component specifies the appropriate application and operating conditions for the SRP/CS designer. The SRP/CS designer should provide information pertaining to their responsibility to apply the basic and well-tried safety principles according to ISO 13849-2:2012, Table C.1 and Table C.2, for the implementation and operation of the hydraulic component.

But if either a) or b) is not achieved, the MTTF_D value for the single hydraulic component should be given by the manufacturer. Instead of using a fixed value for the MTTF_D as described above, it is permissible

to use the B_{10D} concept for $MTTF_D$ of pneumatic, mechanical and electromechanical components also for hydraulic components if the manufacturer can provide data, e.g. B_{10} , B_{10D} , T_{10} , T_{10D} .

C.4 MTTF_D of pneumatic, mechanical and electromechanical components

C.4.1 General

For pneumatic, mechanical and electromechanical components (pneumatic valves, relays, contactors, position switches, cams of position switches) it can be difficult to calculate the $MTTF_D$ for components, which is given in years and which is required by this document. Most of the time, the manufacturers of these kinds of components only give the mean number of cycles until 10 % of the components fail (B_{10}) or fail dangerously (B_{10D}). This clause gives a method for calculating a $MTTF_D$ for components by using B_{10} or T (lifetime) given by the manufacturer related closely to the application dependent cycles.

If all the following criteria are met, the $MTTF_D$ value for a single pneumatic, electromechanical or mechanical component can be estimated according to C.4.2.

- a) The components are designed and manufactured according to basic safety principles in accordance with ISO 13849-2:2012, Table A.1, Table B.1 or Table D.1.

NOTE 1 This information can be found in the data sheet of the component manufacturer.

- b) The components to be used in category 1, 2, 3 or 4 are designed and manufactured according to well-tries safety principles in accordance with ISO 13849-2:2012, Table A.2, Table B.2 or D.2.

NOTE 2 This information can be found in the data sheet of the component manufacturer.

- c) The manufacturer of the component specifies the appropriate application and operating conditions for the SRP/CS designer. The SRP/CS designer should provide information pertaining to their responsibility to fulfil the basic safety principles according to ISO 13849-2:2012, Table A.1, Table B.1 or Table D.1, for the implementation and operation of the component. For category 1, 2, 3 or 4, the user should be informed of their responsibility to fulfil the well-tries safety principles according to ISO 13849-2:2012, Table A.1, Table B.2 or Table D.2, for the implementation and operation of the component.

C.4.2 Calculation of $MTTF_D$ for components from B_{10D}

The mean number of cycles until 10 % of the components fail dangerously (B_{10D})¹⁾ should be determined by the manufacturer of the component in accordance with relevant product standards for the test methods (e.g. the ISO 19973-series, IEC 60947-4-1, IEC 60947-5-1, IEC 60947-5-5, IEC 61810-2-1). The dangerous failure modes of the component should be defined, e.g. sticking at an end position or change of shifting times. With B_{10D} and n_{op} , the mean number of annual operations, $MTTF_D$ for components can be calculated as:

$$MTTF_D = \frac{B_{10D}}{0,1 \times n_{op}} \quad (C.1)$$

where

$$n_{op} = \frac{d_{op} \times h_{op} \times 3\,600 \text{ s/h}}{t_{cycle}} \quad (C.2)$$

where

h_{op} is the mean operation, in hours per day;

1) If the ratio of dangerous failure (RDF) of B_{10} is not given (e.g. by components manufacturer), 50 % of B_{10} can be used, so $B_{10D} = 2 B_{10}$ is recommended.

d_{op} is the mean operation, in days per year;

t_{cycle} is the mean operation time between the beginning of two successive cycles of the component (e.g. switching of a valve) in seconds per cycle.

The operating life time of the component is limited to T_{10D} , the mean time until 10 % of the components fail dangerously:

$$T_{10D} = \frac{B_{10D}}{n_{op}} \quad (C.3)$$

In case no B_{10D} is given by the manufacturer of the component, it is permitted to determine the B_{10D} by the [Formula \(C.4\)](#)

$$B_{10D} = \frac{B_{10}}{R_{DF}} \quad (C.4)$$

If the ratio of dangerous failures (R_{DF}) given by the component manufacturer is estimated at less than 50 % then T_{10D} value is limited to $T_{10} \times 2$.

When the T_{10D} value for a component is less than the mission time (20 years or less), the manufacturer responsible for the integration of the SRP/CS providing the safety function will inform the user to replace the component at or before the T_{10D} period ends. Limiting the use of components to T_{10D} allows maintaining the expected performance level of the safety function.

C.4.3 Explanation of the formulae

The reliability methods in this document assume that the failure of components is distributed exponentially over time: $F_D(t) = 1 - e^{-\lambda_D t}$. For non-electronic components, a Weibull distribution is more likely, but if the operation time of the components is limited to the mean time until 10 % of the components fail dangerously (T_{10D}) then a constant dangerous failure rate (λ_D) over this operation time can be estimated as

$$\lambda_D = \frac{0,1}{T_{10D}} = \frac{0,1 \times n_{op}}{B_{10D}} \quad (C.5)$$

[Formula \(C.6\)](#) takes into account that with a constant failure rate, 10 % of the components in the assumed application fail after T_{10D} [years], corresponding to B_{10D} [cycle]. To be exact:

$$F_D(t) = 1 - e^{-\lambda_D T_{10D}} = 10 \% \text{ leads to } \lambda_D = -\frac{\ln(0,9)}{T_{10D}} = \frac{0,10536}{T_{10D}} \approx \frac{0,1}{T_{10D}} \quad (C.6)$$

with $MTTF_D = 1/\lambda_D$ for exponential distributions, this yields:

$$MTTF_D = \frac{T_{10D}}{0,1} = \frac{B_{10D}}{0,1 \times n_{op}} \quad (C.7)$$

NOTE All variables used in the formulae are physical quantities expressed as the product of a numerical value and a unit of measurement. The correct application of [Formula \(C.5\)](#), [Formula \(C.6\)](#) and $MTTF_D = 1/\lambda_D$ can require the transformation of “years” to “hours” using 1 year = 8 760 h.

C.4.4 Example

For a pneumatic valve, a manufacturer determines a mean value of 60 million cycles as B_{10D} . The valve is used for two shifts each day on 220 operation days a year. The mean time between the beginnings of two successive switching of the valves is estimated as 5 s. This yields the following values:

— d_{op} of 220 d per year;

- h_{op} of 16 h per day;
- t_{cycle} of 5 s per cycle;
- B_{10D} of 60 000 000 cycles.

With these input data the following quantities can be calculated:

$$n_{op} = \frac{220 \times 16 \times 3\,600}{5s} = 2,53 \times 10^6 \text{ cycles/year} \quad (C.8)$$

$$T_{10D} = \frac{60 \times 10^6}{2,53 \times 10^6} = 23,7 \text{ years} \quad (C.9)$$

$$MTTF_D = \frac{23,7}{0,1} = 237 \text{ years} \quad (C.10)$$

This calculation gives a $MTTF_D$ for the component “high” according to [Table C.5](#). These assumptions are only valid for a restricted operation time of 23,7 years for the valve.

C.5 $MTTF_D$ data of electronic components

C.5.1 General

[Table C.2](#) to [Table C.7](#) indicate some typical average values of $MTTF_D$ for electronic components. The data are extracted from the SN 29500 series database. All data are of general type. Various databases are available (see the non-exhaustive list in the Bibliography) which present $MTTF_D$ values for various electronic components. If the designer of an SRP/CS has other, reliable, specific data on the components used, then the use of that specific data instead is recommended.

The values given in [Table C.2](#) to [Table C.7](#) are valid for an ambient temperature of 40 °C, nominal load for current and voltage. A correction factor for $MTTF_D$ should be used where the electronic components operate outside the stated values for temperature or load (see also the SN 29500 series).

In the $MTTF$ column of the tables, the values from the SN 29500 series are for generic components for all possible failure modes which are not necessarily dangerous failures. In the $MTTF_D$ column, it is typically assumed that not all failures modes lead to a dangerous failure. This depends mainly on the application. A precise way of determining the “typical” $MTTF_D$ for components is to carry out an FMEA. Some components, e.g. transistors used as switches, can have short circuits or interruptions as failure. Only one of these two modes can be dangerous; therefore the “remarks” column assumes only 50 % dangerous failure, which means that the $MTTF_D$ for components is twice the given $MTTF$ value.

C.5.2 Semiconductors

See [Table C.2](#) and [Table C.3](#).

Table C.2 — Transistors (used as switches)

Transistor	Example	MTTF for components years	MTTF _D for components years Typical	Remark
bipolar	TO18, TO92, SOT23	38 052	76 104	50 % dangerous failure
bipolar, low power	TO5, TO39	5 708	11 416	50 % dangerous failure
bipolar, power	TO3, TO220, D-Pack	1 903	3 806	50 % dangerous failure
FET	Junction MOS	22 831	45 662	50 % dangerous failure
MOS, power	TO3, TO220, D-Pack	1 903	3 806	50 % dangerous failure

Table C.3 — Diodes, power semiconductors and integrated circuits

Diode	Example	MTTF for components years	MTTF _D for components years Typical	Remark
general purpose	—	114 155	228 311	50 % dangerous failure
suppressor	—	16 308	32 616	50 % dangerous failure
zener diode $P_{\text{tot}} < 1 \text{ W}$	—	114 155	228 311	50 % dangerous failure
rectifier diodes	—	57 078	114 155	50 % dangerous failure
rectifier bridges	—	11 415	22 831	50 % dangerous failure
thyristors	—	2 283	4 566	50 % dangerous failure
triacs, diacs	—	1 522	3 044	50 % dangerous failure
integrated circuits (programmable and non-programmable)	use manufacturer's data			50 % dangerous failure

C.5.3 Passive components

See [Table C.4](#) to [Table C.7](#).

Table C.4 — Capacitors

Capacitor	Example	MTTF for components years	MTTF _D for components years Typical	Remark
standard, no power	KS, KP, KC, KT, MKT, MKC, MKP, MKU, MP, MKV	57 078	114 155	50 % dangerous failure
ceramic	—	22 831	45 662	50 % dangerous failure
aluminium electrolytic	non-solid electrolyte	22 831	45 662	50 % dangerous failure
aluminium electrolytic	solid electrolyte	38 052	76 104	50 % dangerous failure
tantalum electrolytic	non-solid electrolyte	11 415	22 831	50 % dangerous failure
tantalum electrolytic	solid electrolyte	114 155	228 311	50 % dangerous failure

Table C.5 — Resistors

Resistor	Example	MTTF for components years	MTTF _D for components years Typical	Remark
carbon film	—	114 155	228 311	50 % dangerous failure
metal film	—	570 776	1 141 552	50 % dangerous failure
metal oxide and wire-wound	—	22 831	45 662	50 % dangerous failure
variable	—	3 805	7 610	50 % dangerous failure

Table C.6 — Inductors

Inductor	Example	MTTF for components years	MTTF _D for components years Typical	Remark
for MC application	—	38 052	76 104	50 % dangerous failure
low frequency inductors and transformers	—	22 831	45 662	50 % dangerous failure
main transformers and transformers for switched modes and power supplies	—	11 415	22 831	50 % dangerous failure

Table C.7 — Optocouplers

Optocouplers	Example	MTTF for components years	MTTF _D for components years Typical	Remark
bipolar output	SFH 610	7 610	15 220	50 % dangerous failure
FET output	LH 1056	2 854	5 708	50 % dangerous failure

Annex D (informative)

Simplified method for estimating MTTF_D for each channel

D.1 Parts count method

Use of the “parts count method” serves to estimate the MTTF_D for each channel separately. The MTTF_D values of all single components which are part of that channel are used in this calculation.

NOTE The parts count method is an approximation which always errs on the safe side.

The general [Formula \(D.1\)](#) is

$$\frac{1}{\text{MTTF}_D} = \sum_{i=1}^N \frac{1}{\text{MTTF}_{D_i}} = \sum_{j=1}^{\tilde{N}} \frac{n_j}{\text{MTTF}_{D_j}} \quad (\text{D.1})$$

where

MTTF_D is the mean time to dangerous failure for the complete channel;

MTTF_{D_i}, MTTF_{D_j} is the MTTF_D of each component which has a contribution to the sub-function; The first sum is over each component separately; the second sum is an equivalent, simplified form where all n_j identical components with the same MTTF_{D_j} are grouped together.

The example given in [Table D.1](#) gives a MTTF_D of the channel of 22,4 years, which is “medium” according to [6.1.4](#), [Table 6](#).

Table D.1 — Example of the parts list of a circuit board

j	Component	Units n_j	MTTF _{D_j} years	1/MTTF _{D_j} 1/year	n_j/MTTF_{D_j} 1/year
1	transistors, bipolar, low power (see Table C.2)	2	11 416	0,000 087 6	0, 0,000 175 2
2	resistor, carbon film (see Table C.5)	5	228 311	0,000 004 4	0,000 021 9
3	capacitor, standard, no power (see Table C.4)	4	114 155	0,000 008 8	0,000 035 0
4	relay, value given by the manufacturer ($B_{10D} = 20\,000\,000$ cycles, $n_{op} = 633\,600$ cycles per year)	4	315,7	0,003 167 6	0,012 670 3
5	contactor, value given by the manufacturer ($B_{10D} = 2\,000\,000$ cycles, $n_{op} = 633\,600$ cycles per year)	1	31,6	0,031 645 6	0,031 645 6
$\sum(n_j / \text{MTTF}_{D_j})$					0,044 548 0
MTTF _D = 1 / $\sum(n_j / \text{MTTF}_{D_j})$ [years]					22,4

NOTE 1 This method is based on the presumption that a dangerous failure of any component (worst case estimation) within a channel leads to dangerous failure of the channel. The MTTF_D calculation illustrated by [Table D.1](#) is based upon this.

NOTE 2 In this example, the main influence comes from the contactor. The chosen values for MTTF_D and B_{10D} for this example are based on [Annex C](#). For the example application $d_{op} = 220$ days/year, $h_{op} = 8$ h/day and $t_{cycle} = 10$ s/cycles is assumed, giving $n_{op} = 633\,600$ cycles/year. In general, taking manufacturer's values for MTTF_D and B_{10D} leads to a much better result, that is, a higher MTTF_D for the channel.

NOTE 3 When MTTR (mean time to restoration) can be considered negligible, MTTF can be considered equal to MTBF.

NOTE 4 Where only MTBF values are available, a conversion to MTTF_D values can be done by MTTF_D ≈ 2*MTBF.

D.2 MTTF_D for different channels, symmetrisation of MTTF_D for each channel

The designated architectures of 6.1.3.2 assume that for different channels in a redundant SRP/CS the values for MTTF_D for each channel are the same. This value per channel should be input for Figure 12.

If the MTTF_D of the channels differ, there are two possibilities:

- as a worst-case assumption, the lower value should be taken into account;
- Formula (D.2) can be used as an estimation of a value that can be substituted for MTTF_D for each channel:

$$MTTF_D = \frac{2}{3} \left[MTTF_{D\ C1} + MTTF_{D\ C2} - \frac{1}{\frac{1}{MTTF_{D\ C1}} + \frac{1}{MTTF_{D\ C2}}} \right] \quad (D.2)$$

where

MTTF_{D C1} and MTTF_{D C2} are the values for two different redundant channels each limited to a maximum value of 100 years (categories B, 1, 2 and 3) or 2 500 years (category 4).

EXAMPLE One channel has an MTTF_{D C1} = 3 years, the other channel has an MTTF_{D C2} = 100 years, then the resulting MTTF_D = 66 years for each channel. This means a redundant system with 100 years MTTF_D in one channel and 3 years MTTF_D in the other channel is equal to a system where each channel has a MTTF_D of 66 years.

A redundant system with two channels and different MTTF_D values for each channel can be substituted by a redundant system with identical MTTF_D in each channel by using the above formula. This procedure is necessary for the correct use of Figure 12.

NOTE This method assumes independent parallel channels.

Annex E (informative)

Estimates for diagnostic coverage (DC) for functions and subsystems

E.1 Examples of diagnostic coverage (DC)

See [Table E.1](#).

Table E.1 — Estimates for diagnostic coverage (DC)

Measure	DC ^{a,b}
Input device	
cyclic test stimulus by dynamic change of the input signals	90 %
plausibility check, e.g. use of normally open and normally closed mechanically linked contacts	99 %
cross monitoring of inputs without dynamic test	percentage to be defined depending on the specific application, e.g. depending on how often a signal change is done by the application (see NOTE 4)
cross monitoring of input signals with dynamic test if short circuits are not detectable (for multiple I/O)	90 %
cross monitoring of input signals and intermediate results within the logic (L), and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O)	99 %
indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of machine actuators)	90 % to 99 %, depending on the application (see NOTE 2)
direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99 %
fault detection by the process	percentage to be defined depending on the specific application; this measure alone is not sufficient for the required performance level (PL _r) e (see NOTES 2, 3 and 5)
monitoring some characteristics of the sensor (response time, range of analogue signals, e.g. electrical resistance, capacitance)	60 %
Logic	
indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of machine actuators, plausibility check of final result)	90 % to 99 %, depending on the application (see NOTE 2)
direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements, plausibility check of intermediate results)	99 %
simple temporal time monitoring of the logic (e.g. timer as watchdog, where trigger points are within the program of the logic)	60 %
temporal and logical monitoring of the logic by the watchdog, where the test equipment does plausibility checks of the behaviour of the logic	90 %

Table E.1 (continued)

Measure	DC ^{a,b}
start-up self-tests to detect latent faults in parts of the logic (e.g. program and data memories, input/output ports, interfaces)	60 % to 90 % (see NOTE 2)
checking the monitoring device reaction capability (e.g. watchdog) by the main channel at start-up or whenever the safety function is demanded or whenever an external signal demand it, through an input facility	90 %
dynamic principle (all components of the logic are required to change the state ON-OFF-ON when the safety function is demanded), e.g. interlocking circuit implemented by relays	99 %
invariable memory: signature of one word (single bus width)	90 %
invariable memory: signature of double word (double bus width)	99 %
variable memory: RAM-test by use of redundant data e.g. flags, markers, constants, timers and cross comparison of these data	60 %
variable memory: check for readability and write ability of used data memory cells	60 %
variable memory: RAM self-test (e.g. "galpat" or "Abraham") or double RAM with hardware or software comparison and read/write test.	99 %
processing unit: self-test by software (see IEC 61508-7:2010, A.3)	60 % to 90 % (see NOTE 2)
processing unit: coded processing (see IEC 61508-7:2010, A.3)	90 % to 99 % (see NOTE 2)
fault detection by the process	percentage to be defined depending on the specific application; this measure alone is not sufficient for the required performance level (PL _r) e (see NOTES 2, 3 and 5)
Output device	
monitoring of outputs by one channel without dynamic test	percentage to be defined depending on the specific application, e.g. depending on how often a signal change is done by the application (see NOTE 4)
cross monitoring of outputs without dynamic test	percentage to be defined depending on the specific application, e.g. depending on how often a signal change is done by the application (see NOTE 4)
cross monitoring of output signals with dynamic test without detection of short circuits (for multiple I/O)	90 %
cross monitoring of output signals and intermediate results within the logic (L) and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O)	99 %
redundant shut-off path with monitoring of the outputs by logic and test equipment, see example ISO 13849-2:2012, Annex E	99 %
indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of machine actuators)	90 % to 99 %, depending on the application (see NOTE 2)
fault detection by the process	percentage to be defined depending on the specific application; this measure alone is not sufficient for the required performance level (PL _r) e (see NOTES 2, 3 and 5)
direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99 %

Table E.1 (continued)

Measure	DC ^{a,b}
NOTE 1 For additional estimations for DC, see, e.g. IEC 61508-2:2010, Table A.2 to Table A.14.	
NOTE 2 For measures where a DC range is given (e.g. fault detection by the process) the correct DC value can be determined by considering all dangerous failures and then deciding which of them are detected by the DC measure. In case of any doubt a FMEA should be the basis for the estimation of the DC.	
NOTE 3 For the DC measure “Fault detection by the process” the demand rate of the safety function (r_d) and the process diagnostic (test) rate (r_t) can be considered together with a limitation of the effective DC of the tested component:	
a) $r_t/r_d > 1$	DC is limited to 60 %
b) $r_t/r_d > 10$	DC is limited to 90 %
c) $r_t/r_d > 100$	DC is limited to 99 %
NOTE 4 For the DC measure “Cross monitoring of inputs or outputs without dynamic test”, the effect of the test rate can be incorporated using the following limitations for the effective DC of the tested component:	
For Category 3 and 4:	
— $r_t < 1/\text{year}$	DC is 0 %
— $r_t \geq 1/\text{year}$	DC is limited to 90 %
— $r_t \geq 1/\text{month}$	DC is limited to 99 %
NOTE 5 When the DC measure “fault detection by the process” is combined with other DC measures as listed in Annex E this measure can still be included in the DC estimation of the block, even for PLr e.	
^a DC measures can be combined to achieve a higher DC.	
^b If medium or high DC is claimed for the logic, at least one measure for each of variable memory, invariable memory and processing unit with each DC at least 60 % shall be applied. Other measures can be used than those listed in this table.	

For the application of [Table E.1](#) see the indicative examples below.

EXAMPLE 1 ISO 13849-2:2012, Annex E presents a complete worked example (which is very detailed) for the validation of fault behaviour and diagnostic means on an automatic assembly machine.

NOTE ISO/TR 24119 describes a pragmatic step-by-step table-based methodology for evaluation of DC for series connected interlocking devices with potential free contacts.

EXAMPLE 2 The DC measure “fault detection by the process” can only be applied if the safety-related component is involved in the production process, e.g. a standard PLC or standard sensors are used for workpiece processing and as part of one of two channels executing the safety function. The appropriate DC level depends on the overlap of the commonly used resources (logic, inputs/outputs). For example, when all faults of a rotary encoder on a printing machine lead to highly visible interruption of the printing process, the DC for this sensor used to monitor a safely limited speed can be estimated as 90 % up to 99 %.

E.2 Estimation of the average diagnostic coverage

In many systems, several measures for fault detection can be used. These measures can check different parts of the SRP/CS and have different DC. For an estimation of the PL according to [6.1.8](#) and [Figure 12](#) only one average DC for the whole SRP/CS performing the safety function is applicable.

DC may be determined as the ratio between the failure rate of detected dangerous failures and the failure rate of total dangerous failures. According to this definition an average diagnostic coverage DC_{avg} is estimated by [Formula \(E.1\)](#):

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \dots + \frac{DC_N}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \dots + \frac{1}{MTTF_{DN}}} \quad (E.1)$$

All components of the SRP/CS without fault exclusion should be considered and summed up. For each block, the $MTTF_D$ and the DC are taken into account. DC in this formula means the ratio of the failure rate of detected dangerous failures of the part (regardless of the measures used to detect the failures) to the failure rate of all dangerous failures of the part. Thus, DC refers to the tested part and not to the testing device. Components without failure detection (e.g. which are not tested) have $DC = 0$ and contribute only to the denominator of DC_{avg} .

Annex F (informative)

Method for quantification of measures against common cause failures (CCF)

F.1 General

The comprehensive procedure for measures against CCF as described in [F.2](#) and [F.3](#) should be followed for each subsystem of category 2, 3 or 4 which contributes to the SRP/CS.

The simplified procedure in [6.1.8](#) of this document assumes a β -factor of 20% according to IEC 61508-6:2010, Annex D. This can be reached by following the procedure in [F.2](#).

The measures described in [F.2](#) and [F.3](#) should be documented in order to support a minimum score of 65 points is achieved.

F.2 Estimation of effect of measures against CCF

Every part of the subsystem should be considered for CCF.

[Table F.1](#) lists the measures, based on engineering judgement, which represent the contribution each measure makes in the reduction of CCFs.

In [F.3](#) the measures are described in detail. For each listed measure, the full score can only be claimed, if the measure is fully implemented. If a measure is only partly fulfilled a score of zero should be assumed.

Each measure should be evaluated based on the specific application and the relevant causes for CCF (e.g. for electronic systems only “prevention of EMI” is relevant and not “impurity of fluidic medium”).

If components are used in the SRP/CS that are not sufficiently protected against over-voltage, environmental influences by internal measures this protection should be reached on system level using external protection components, filters, shielding.

Table F.1 — Scoring process and quantification of measures against CCF

No.	Measure against CCF	Score
1	separation/segregation	15
2	diversity	20
3	design/application/experience	
3.1	protection against over-voltage, over-pressure, over-current, over-temperature	15
3.2	components used are well-tried	5
4	assessment/analysis	5
5	training	5
6	environmental	
6.1	prevention of EMI or impurity of fluidic medium	25
6.2	other influences	10
	total	[max. achievable 100]
Total score		Measures for avoiding CCF
65 or better		Meets the requirements
Less than 65		Process failed ⇒ apply additional measures

The measures listed in [Table F.1](#) should be evaluated according to their effectiveness to avoid or control CCFs of redundant channels. Engineering judgement should support that typical causes for CCF are reduced as much as reasonably possible.

NOTE 1 The calculation of the CCF is usually performed on a subsystem level, as the measures for the individual subsystems differ (e.g. inputs, logic and outputs).

NOTE 2 Redundant channels in this annex means functional channel and testing channel in category 2 or redundant functional channels in categories 3 and 4.

NOTE 3 Typical CCF causes are over-voltage, over-pressure, over-current, over-temperature, humidity, shock, vibration, EMI, impurity of the pressure medium. The appropriate level of these causes is deduced from the expected application of the SRP/CS including foreseeable faults (e.g. failure of a cooling fan) and reasonably foreseeable misuse. The measures can vary for different categories (category 2 vs. 3 and 4) or input/logic/output parts of the SRP/CS.

F.3 Description of the measures against common cause failure (CCF) in [Table F.1](#)

F.3.1 Separation/segregation

Physical separation between signal paths of redundant channels, for example:

- separation in wiring (e.g. multi conductor cable with suitable insulation between conductors);
- separation in piping (e.g. avoiding damaging of a hydraulic pipe due to high pressure released from another adjacent pipe);
- detection of short circuits and open circuits in cables by dynamic test;
- separate shielding for the signal path of each channel;
- redundant channels on separate printed-circuit boards or in separate housings or cabinets;
- sufficient clearances and creepage distances between redundant channels on printed-circuit boards, also taking into account e.g. tin whiskers (see ISO 13849-2:2012, D.2.2).

F.3.2 Diversity

Diversity considerations include, for example:

- a) Different technologies/design or physical principles are used, for example:
 - first channel electronic or programmable electronic and second channel electromechanical hardwired;
 - different initiation of safety function for each channel (e.g. position, pressure, temperature);
 - first channel valve with rubber seal and second channel with metal seal;
 - two position switches are used to detect the opening of a movable guard (safety guard), the first one is operated when the safety guard is opened and uses a break-contact element with direct opening action in accordance with IEC 60947-5-1:2020 Annex K, the second one is operated when the safety guard is closed and uses a make-contact element;
- b) Sensing elements employ different measurement principles (e.g. digital and analogue) or physical principles (e.g. distance, pressure or temperature);
- c) Different components, e.g. of different manufacturers (not re-badged);
- d) Different loads, e.g. contact/valve of one channel switches without load, contact/valve in the second channel switches under load.

F.3.3 Design/application/experience

Protection against or control of over-voltage, over-pressure, over-current, over-temperature, for example:

- a) Inputs and outputs of the SRP/CS and the power supply of the logic are protected from potential levels of over-voltage and/or over-current (see also IEC 60204-1);

NOTE Parts of the SRP/CS are capable of withstanding or are protected from potential levels of either over-voltage or over-current, or both. Possible maximum over-voltage level of SW mode PSU (switch mode power supply) depends on the applied standard (e.g. maximum voltages limit under single fault condition).

It is important to take into account the possible maximum over-voltage level by applied standard SW mode PSU as well as other operating conditions (e.g. over-voltage category, operating temperature).

- b) The measure against over-pressure can be a single channel system if the primary pressure in case of failure can never rise over the operating pressure multiplied by 1,5. ISO 4414 defines a requirement for protection from unintended pressure (e.g. a pressure relief valve).

Only well-tried components are used. See [6.1.11](#) and ISO 13849-2.

F.3.4 Assessment/analysis

For each part of SRP/CS a failure mode and effect analysis or FTA has been carried out to identify potential causes for CCF and its results are taken into account to avoid CCFs in the design.

F.3.5 Training

Designers have been trained (with training documentation, e.g. certificate of training) to understand the causes and consequences of CCFs.

F.3.6 Environmental

F.3.6.1 Prevention of EMI or impurity of the pressure medium

For electrical/electronic systems, contamination and electromagnetic disturbances are prevented to protect against CCFs in accordance with appropriate standards (e.g. IEC 61326-3-1, IEC 61000-6-7:2014, IEC 61000-1-2:2016, IEC 61800-5-2).

NOTE 1 These EMI standards usually have more stringent requirements than standard components (e.g. general-purpose PLC) are designed to meet. See IEC 61800-3 for further information.

NOTE 2 [Annex L](#) provides further guidance in relation to EMI immunity.

For fluidic systems, filtration of the pressure medium, prevention of dirt intake, drainage of compressed air, is implemented in conformity with the component manufacturers' requirements concerning purity of the pressure medium (see ISO 8573-1 for guidance).

For combined fluidic and electric systems, both aspects should be considered.

F.3.6.2 Other influences

The SRP/CS is immune to all relevant environmental influences such as temperature, shock, mechanical stresses, vibration, humidity, as specified in relevant standards, e.g. the IEC 60068 series, taking into account the increased requirements for safety-related applications.

F.4 Measures against common cause failure (CCF) and other relevant standards

For some SRP/CS (subsystems) not all the measures against CCF listed in [Table F.1](#) can provide an appropriate reduction of the CCF impact since the potential risk reduction that can be provided by those SRP/CS is limited also by their systematic capabilities (e.g. detection principle of sensors).

NOTE Some relevant standards (e.g. the IEC 62024 series for the application of protecting equipment to detect the presence of persons or ISO 14119:2013 for the selection and application of interlocking devices associated with guards) can include application limits related to systematic capabilities.

The designer of the complete SRP/CS applies the measures stated in these standards and conforms with the instructions for use provided by the manufacturer.

Annex G (informative)

Systematic failure

G.1 General

This annex provides guidance on measures to control and avoid systematic failures during the design and integration of SRP/CS.

G.2 Measures for the control of systematic failures

The following measures should be applied:

- a) Use of de-energization: The SRP/CS should be designed so that the machine will achieve or maintain a safe state upon a power supply loss (see ISO 13849-2:2012, IEC 60204-1:2016+AMD1:2021, 7.5 and ISO 62061:2021).
- b) Measures for controlling the effects of voltage breakdown, voltage variations, overvoltage, undervoltage: SRP/CS behaviour in response to voltage breakdown, voltage variations, overvoltage, and undervoltage conditions should be predetermined so that the SRP/CS can achieve or maintain a safe state of the machine (see also IEC 60204-1:2016+AMD1:2021, Clause 7 and IEC 61508-7:2010, A.8).
- c) Measures for controlling or avoiding the effects of the physical environment (e.g. temperature, humidity, water, vibration, dust, corrosive substances, EMI and its effects): SRP/CS behaviour in response to the effects of the physical environment should be predetermined so that the SRP/CS can achieve or maintain a safe state of the machine (see also, for example, IEC 60529, IEC 60204-1).
- d) Program sequence monitoring should be used with SRP/CS containing software in order to detect defective program sequences: A defective program sequence exists if the individual elements of a program (e.g. software modules, subprograms or commands) are processed in the wrong sequence or period of time or if the clock of the processor is faulty (see IEC 61508-7:2010, A.9).
- e) Measures for controlling the effects of errors and other effects arising from any data communication process (see IEC 61508-2:2010, 7.4.11)

In addition, one or more of the following measures should be applied, taking into account the complexity of the SRP/CS and its PL:

- failure detection by automatic tests;
- tests by redundant hardware;
- diverse hardware;
- operation in the positive mode;
- mechanically linked contacts;
- direct opening action;
- oriented mode of failure;
- over-dimensioning by a suitable factor, where the manufacturer can demonstrate that over-dimensioning improves reliability.

NOTE For examples for over-dimensioning see ISO 13849-2:2012, Table D.2.

G.3 Measures for avoidance of systematic failures during SRP/CS design

The following measures should be applied:

- a) Use of suitable materials and adequate manufacturing;
Selection of material, manufacturing methods and treatment in relation to, e.g. stress, durability, elasticity, friction, wear, corrosion, temperature, conductivity, dielectric rigidity.
- b) Correct dimensioning and shaping;
Consideration of, e.g. stress, strain, fatigue, temperature, surface roughness, tolerances, manufacturing.
- c) Proper selection, combination, arrangements, assembly and installation of components, including cabling, wiring and any interconnections;
Apply appropriate standards and manufacturer's application notes, e.g. catalogue sheets, installation instructions, specifications, and use of good engineering practice.
- d) Compatibility;
Use components with compatible operating characteristics.
NOTE Components such as hydraulic or pneumatic valves can require cyclic switching to avoid failure by non-switching or unacceptable increase in shifting times. In this case a periodic test is necessary.
- e) Withstanding specified environmental conditions;
Design the SRP/CS so that it is capable of working in all expected environments and in any foreseeable adverse conditions, e.g. temperature, humidity, vibration and EMI (see ISO 13849-2:2012, D.2).
- f) Use of components designed to an appropriate standard and having well-defined failure modes.
To reduce the risk of undetected faults by the use of components with specific characteristics see IEC 61508-7:2010, B.3.3.

In addition, one or more of the following measures should be applied, taking into account the complexity of the SRP/CS and its PL:

- Hardware design review (e.g. by inspection or walk-through);
To reveal by reviews and analysis discrepancies between the specification and implementation.
- Computer-aided design tools capable of simulation or analysis;
Perform the design procedure systematically and include appropriate automatic construction elements that are already available and tested.
- Simulation.
Perform a systematic and complete inspection of an SRP/CS design in terms of both the functional performance and the correct dimensioning of their components.

G.4 Measures for avoidance of systematic failures during SRP/CS integration

The following measures should be applied during integration of the SRP/CS:

- functional testing;

- project management;
- documentation.

In addition, black-box testing should be applied, taking into account the complexity of the SRP/CS and its PL.

G.5 Management of functional safety

A functional safety plan should be drawn up and documented for each SRP/CS design project and should be updated as necessary. The functional safety plan is intended to provide measures for preventing incorrect specification, implementation, or modification issues.

The functional safety plan should identify the relevant activities (see [Figure 4](#)) and should be adapted to the project.

NOTE 1 The functional safety plan can be part of other design documents.

NOTE 2 The content of the functional safety plan depends upon the specific circumstances, which can include:

- size of project;
- degree of complexity;
- degree of novelty of design and technology;
- degree of standardization of design features;
- possible consequence(s) in the event of failure.

In particular, the functional safety plan should:

- identify the relevant activities in the SRP/CS design process (specification, design, integration, analysis, testing, verification, validation) and details of when they should take place;
- identify the roles and resources necessary for carrying out and reviewing each of these activities;
- identify procedures for release, configuration, documentation and modification of hardware and software design;
- establish a validation plan (see [10.1.2](#));
- identify relevant activities before carrying out any modification.

NOTE 3 The request for a modification can arise from, for example:

- SRS change;
- conditions of actual use;
- incident/accident experience;
- change of material processed;
- obsolescence;
- modifications of the machine or of its operating modes.

The effect of the requested modification should be analysed to establish the effect on the safety function.

All accepted modifications that have an effect on the SRP/CS should initiate a return to an appropriate design phase for its hardware and/or for its software (e.g. specification, design, integration, installation, commissioning, and validation). All subsequent phases and management procedures should then be

carried out in accordance with the procedures specified for the specific phases in this document. All relevant documents should be revised, amended and reissued accordingly.

STANDARDSISO.COM : Click to view the full PDF of ISO 13849-1:2023

Annex H (informative)

Example of a combination of several subsystems

[Figure H.1](#) is a schematic diagram of the combination of subsystems of an SRP/CS providing one of the safety functions controlling a machine actuator. This is not a functional/working diagram and is included only to demonstrate the principle of combining categories and technologies in this one function.

The control is provided through electronic control logic and a hydraulic directional control valve. The risk is reduced by an AOPD, which detects access to the hazard zone and prevents start-up of the fluidic actuator when the light beam is interrupted.

The subsystems of the SRP/CS which provide the safety function are: AOPD, electronic control logic, hydraulic directional control valve and their interconnecting means.

These combined subsystems provide a stop function as a safety function. As the AOPD is interrupted, the outputs transfer a signal to the electronic control logic, which provides a signal to the hydraulic directional control valve to stop the hydraulic flow as the output of the SRP/CS. At the machine, this stops the hazardous movement of the fluidic actuator.

This combination of subsystems creates a safety function demonstrating the combination of different categories and technologies based on the requirements given in [Clause 6](#). Using the principles given in this document, the subsystems shown in [Figure H.2](#) can be described as follows.

- Category 2, PL c, PFH = $1,5 \times 10^{-6}/\text{h}$ for the electro-sensitive protective device (light barrier). To reduce the probability of faults this device uses well-tried safety principles;
- Category 3, PL d, PFH = $2,0 \times 10^{-7}/\text{h}$ for the electronic control logic. To increase the level of safety performance of this electronic control logic, the structure of this subsystem is redundant and implements several fault detection measures such that it is able to detect most of single faults;
- Category 1, PL c, PFH = $1,1 \times 10^{-6}/\text{h}$ for the hydraulic directional control valve. The status of being well-tried is mainly application-specific. In this example, the valve is considered to be well-tried. In order to reduce the probability of faults, this device comprises well-tried components applied using well-tried safety principles and all application conditions are considered (see [6.1.3.2.3](#)).

NOTE 1 The position, size and layout of the interconnecting means have also to be taken into account.

This combination leads to a summed-up value of PFH = $2,8 \times 10^{-6}/\text{h}$ in the range of PL c. Together with the lowest PL of all three subsystems PL_{low} c a leads to an overall performance level of PL c (see [6.2](#)).

NOTE 2 In case of one fault in the category 1 or the category 2 subsystem of [Figure H.2](#) there can be a loss of the safety function.

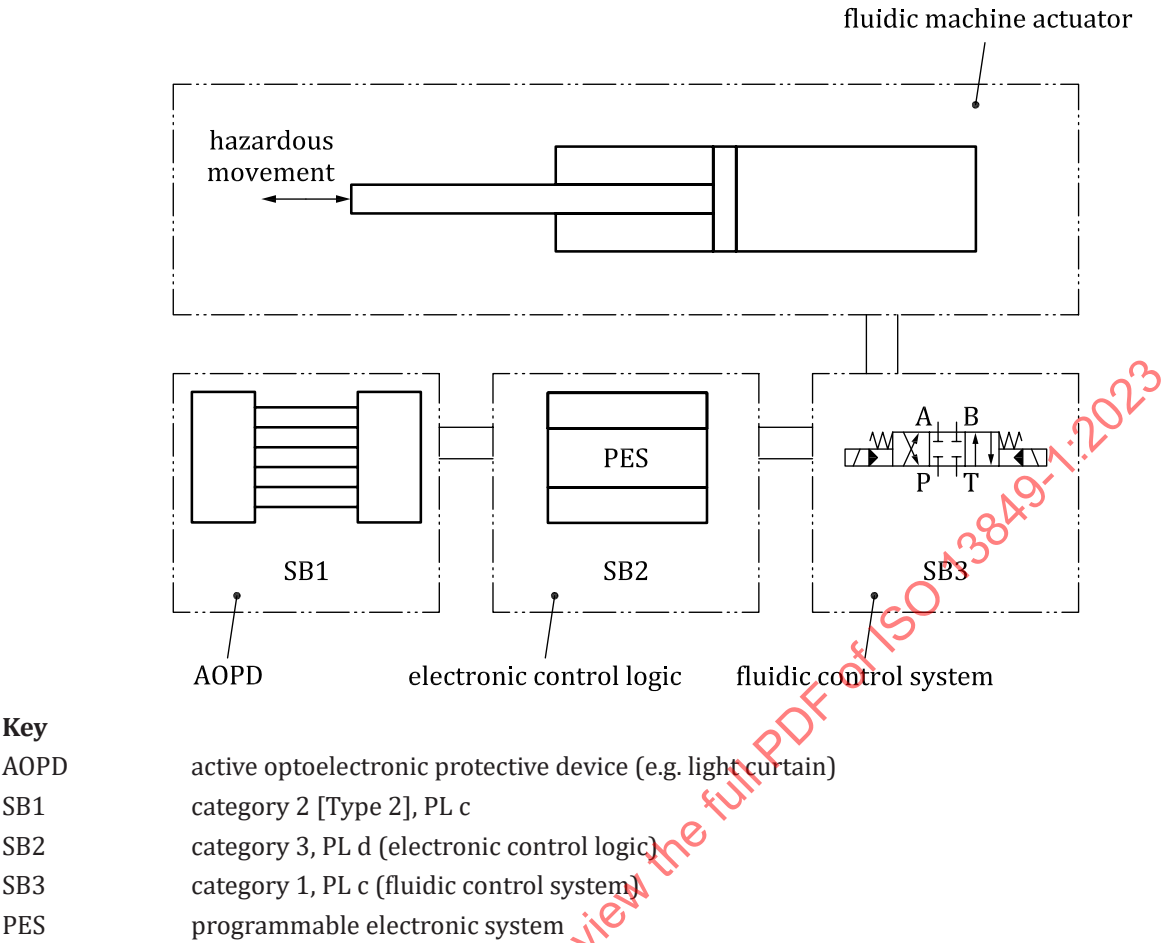
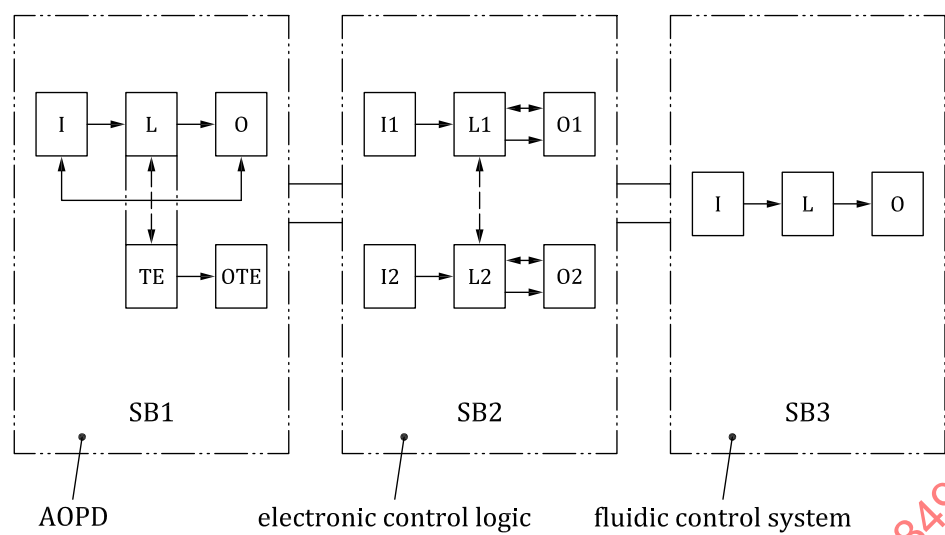


Figure H.1 — Example — Block diagram explaining combination of subsystems



- Key**
- AOPD active optoelectronic protective device (e.g. light curtain)
 - I, I1, I2 input devices, e.g. sensor
 - L, L1, L2 logic
 - O, O1, O2, OTE output devices, e.g. main contactor
 - SB1 category 2 [Type 2], PL c
 - SB2 category 3, PL d (electronic control logic)
 - SB3 category 1, PL c (fluidic control system)
 - TE test equipment

Figure H.2 — Substitution of [Figure H.1](#) by designated architectures

Annex I (informative)

Examples for the simplified procedure to estimate the PL of subsystems

I.1 General

This annex illustrates the use of the simplified procedure for estimating PL given in 6.1.8 and the preceding annexes for identifying safety functions and determining the PL. The quantification of two control circuits is given. For the stepwise procedure, see Figure 4.

The following examples do not take into account the measures to ensure systematic integrity, software requirements, and the correct application of basic and well-tried principles. They are only intended to show quantification of $MTTF_D$, DC_{avg} , CCF, category and corresponding PL.

Two examples (A and B) of control circuits for different machines are examined (see Figure I.1 and Figure I.3). Both illustrate the performance of the same safety function of the interlocking of the guard door, but they have different PL_r due to differences in the applications. The first example consists of one channel of electromechanical components with medium and high $MTTF_D$ values, while the second example is made up of two channels, one electromechanical and the other programmable electronic, of components with medium and high $MTTF_D$ values, and with appropriate diagnostic testing.

I.2 Safety function and required performance level (PL_r)

For both examples, the requirements of the safety function associated with the guard door interlocking can be specified as follows.

The dangerous movement will be stopped (by decelerating or de-energising the electric motor) when the interlocking guard is opened.

NOTE For the example B, the risk assessment determined that a loss of controlled deceleration of the motor as a result of a malfunction (SW2, CC or PLC) was acceptable.

The minimum distance between the interlocking guard and moving parts of the machine was determined according to ISO 13855:2010, based on the machine stopping performance.

For example, A, the risk parameters according to the risk graph method (see Figure A.1) are as follows:

- severity of injury, $S = S2$, serious;
- frequency and/or exposure time to hazard, $F = F1$, seldom to less often and/or the exposure time is short;
- possibility of avoiding or limiting harm, $P = P1$, possible under specific conditions.

These risk parameter selections lead to a PL_r of c.

Determination of the preferred category: a performance level of “c” can be achieved typically by very reliable single-channel systems (category 1), tested single-channel systems (category 2) or redundant architectures (category 3) (see Figure 12).

For example, B, the risk parameters $S2$ and $P1$ are the same, but for frequency and/or exposure time to hazard, $F = F2$, frequent to continuous and/or the exposure time is long.

These decisions lead to a PL_r of d.

Determination of the preferred category: a performance level of “d” can be achieved typically by redundant architectures (category 2 or 3) (see [Figure 12](#)).

I.3 Example A — Single-channel system

I.3.1 Identification of safety-related parts

All components contributing to the guard interlocking safety function are represented in [Figure I.1](#). Other components that do not contribute to the safety function (e.g. start and stop switches) are omitted for simplicity.

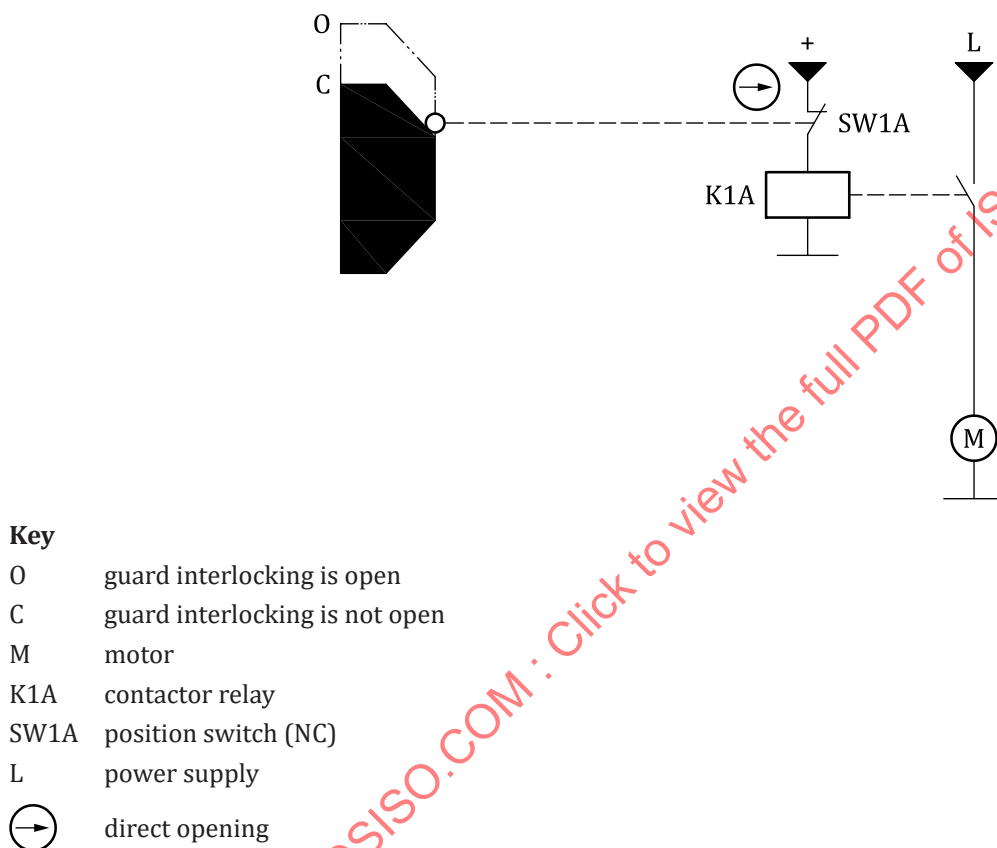


Figure I.1 — Control circuit A for performing safety function

In this example, a position switch SW1A with direct opening action is used in the positive mode of actuation but no-fault exclusion is justified for the mechanical parts. The position switch is connected to a contactor relay K1A, which is able to switch off the power to the motor. The key features of these SRP/CS are therefore:

- one channel of electromechanical components;
- position switch SW1A (NC) has direct opening action of the contact and high B_{10D} ;
- contactor relay K1A has high B_{10D} .

The position switch and contactor relay in this example are both well-tried components when implemented according to ISO 13849-2:2012.

The SRP/CS can be illustrated in a safety-related block diagram as shown in [Figure I.2](#).

**Key**

SW1A position switch

K1A contactor relay

Figure I.2 — Safety-related block diagram identifying safety-related parts (SRPs) of example A**I.3.2 Quantification of $MTTF_D$, DC_{avg} , measures against CCF, category and performance level**

The values for $MTTF_D$, DC_{avg} and measures against CCF are assumed to be estimated according to [Annex C](#), [Annex D](#), [Annex E](#) and [Annex F](#), or to be given by the manufacturer. The categories are estimated according to [6.1.3](#).

— $MTTF_D$

The position switch SW1A and the contactor relay K1A contribute to the $MTTF_D$ of the one channel. The values of $B_{10D,SW1A} = 20\,000\,000$ cycles (position switch independent of load) and $B_{10D,K1A} = 400\,000$ cycles (contactor relay with maximum load) are assumed to be provided by the manufacturer. Applying the method of [C.4.2](#) with 220 working days per year, 8 working hours per day and a cycle time of 60 min gives $MTTF_{D,SW1A} = 113\,636$ years and $MTTF_{D,K1A} = 2\,273$ years. Then using the parts count method of [D.1](#), the $MTTF_D$ of the one channel is calculated as:

$$\frac{1}{MTTF_D} = \frac{1}{MTTF_{D,SW1A}} + \frac{1}{MTTF_{D,K1A}} = \frac{1}{113\,636 \text{ years}} + \frac{1}{2\,273 \text{ years}} = \frac{0,000\,45}{\text{year}} \quad (I.1)$$

which gives $MTTF_D = 2\,222$ years (limited to 100 years) for the channel, which is “high” according to [6.1.4](#), [Table 6](#).

NOTE If no B_{10D} information for SW1A or K1A is available, a worst-case assumption according to [C.2](#) or [C.4](#) can be made.

— T_{10D}

The method given in [C.4.2](#) gives $T_{10D,SW1A}$ of 11 364 years and $T_{10D,K1A}$ of 227 years, which both exceed the mission time of 20 years and therefore eliminate the need for any preventive exchange.

— DC

No diagnostic testing is performed in control circuit A, the $DC = 0$ or “none”, as only one channel is used, DC is not relevant.

— CCF

As only one channel is used, measures against CCF are not relevant.

— Category

The characteristics of category 1 (basic and well-tried safety principles, well tried components) are fulfilled, including the requirement for the $MTTF_D$ of the channel to be “high”.

Input data for [Figure 12](#): $MTTF_D$ of the channel is “high” (100 years), DC_{avg} is “none” and category is 1.

Using [Figure 12](#), this is interpreted as performance level c.

Application of [Annex K](#) gives an PFH of $1,14 \times 10^{-6}/h$ and PL c.

This result matches the $PL_r c$ according to [Figure I.2](#). The control system of example A therefore satisfies the requirements for risk reduction of the example A application of [I.2](#), with S2, F1, P1 and $PL_r c$.

I.4 Example B — Redundant system

I.4.1 Identification of safety-related parts

All components contributing to the guard interlocking safety function are represented in [Figure I.3](#). Other components that do not contribute to the safety function (for example, start and stop switches or delayed switching of K1B) are omitted for simplicity.

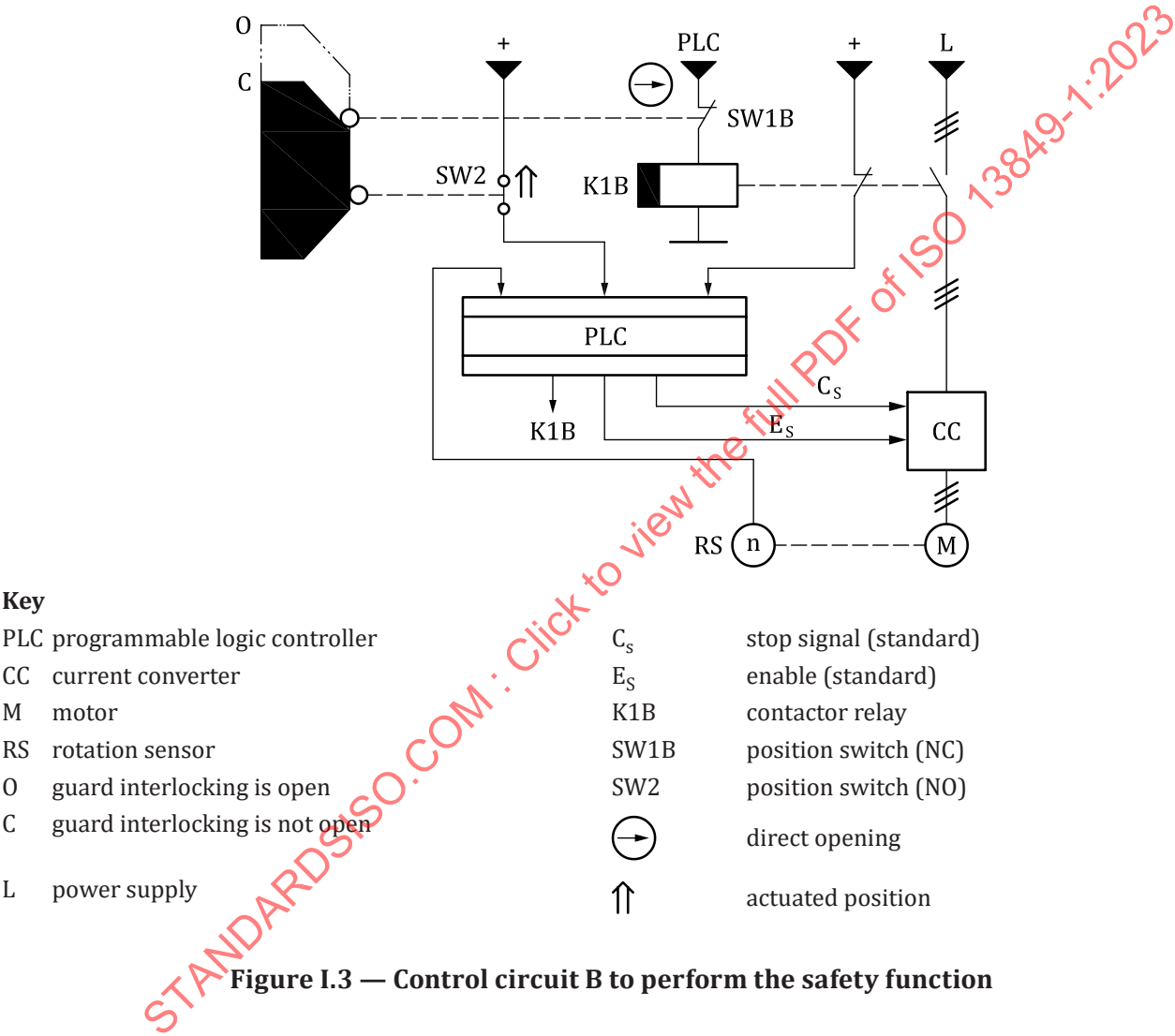


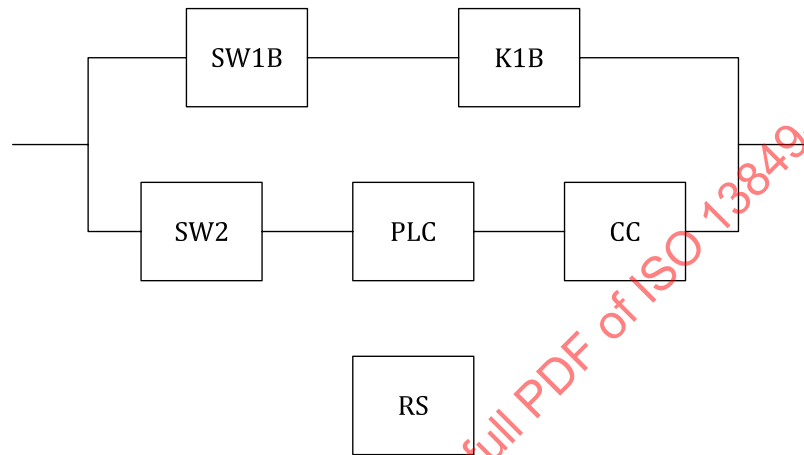
Figure I.3 — Control circuit B to perform the safety function

In this second example, a two-channel architecture is used to provide redundancy. As in example A, the first channel includes a position switch SW1B with direct opening action used in the positive mode of actuation. This position switch is connected to a contactor relay K1B, which is able to switch off the power to the motor. In the second channel, which includes (programmable) electronic components, a second position switch SW2 is connected to a programmable logic controller PLC that can command the current converter CC to switch off the power to the motor. The key features of these SRP/CS are therefore:

- redundant channels, one electromechanical and the other programmable electronic;
- only position switch SW1B (NC) has direct opening action of the contact, but both position switches SW1B and SW2 have high B_{10D} ;

- contactor relay K1B has high $MTTF_D$;
- electronic components PLC and CC have medium $MTTF_D$;
- the SRASW of the PLC, e.g. the part of the software related to the monitoring of the input signals SW2, K1B, RS and the outputs commands to the current converter, is specified, designed and verified according to 7.3 for a PL_r of d.

The SRP/CS and their division into channels can be illustrated in a safety-related block diagram as shown in Figure I.4. The first channel therefore consists of SW1B and K1B and the second channel consists of SW2, PLC and CC, while RS is only used to test the current converter.



Key

SW1B position switch
K1B contactor relay
SW2 position switch

PLC programmable logic controller
CC current converter
RS rotation sensor

Figure I.4 — Block diagrams identifying safety-related parts (SRPs) of example B

I.4.2 Quantification of $MTTF_D$ for each channel, average diagnostic coverage, measures against CCF, category and performance level

The values for $MTTF_D$ for each channel, DC_{avg} and measures against CCF are assumed to be evaluated according to Annex C, Annex D, Annex E and Annex F, or to be provided by the manufacturer. The categories are determined according to 6.1.3.

The position switch SW1B has a direct opening action and is used in the positive mode of actuation but no-fault exclusion is justified for the mechanical parts.

- $MTTF_D$

The position switch SW1B and contactor relay K1B contribute to the $MTTF_{D,C1}$ of the first channel. The values of $B_{10D,SW1B} = 20\,000\,000$ cycles (position switch independent of load) and $B_{10D,K1B} = 400\,000$ cycles (contactor relay with maximum load) are assumed to be provided by the manufacturer. Applying the method of C.4.2 with 300 working days per year, 16 working hours per day and a cycle time of 4 min gives $MTTF_{D,SW1B} = 2\,778$ years and $MTTF_{D,K1B} = 56$ years. Then using the parts count method of D.1, the $MTTF_{D,C1}$ of the first channel is calculated as

$$\frac{1}{MTTF_{D,C1}} = \frac{1}{MTTF_{D,SW1B}} + \frac{1}{MTTF_{D,K1B}} = \frac{1}{2\,778 \text{ years}} + \frac{1}{56 \text{ years}} = \frac{0,018\,2}{\text{year}} \quad (I.2)$$

which gives an $MTTF_D = 55$ years for the channel, which is “high” according to 6.1.4 and Table 6.

In the second channel SW2, PLC and CC contribute to $MTTF_{D,C2}$. The $B_{10D,SW2}$ of 1 000 000 cycles is assumed to be given by the manufacturer. Applying the method of C.4.2 as for the first channel gives an $MTTF_{D,SW2}$ of 139 years. For PLC and CC an $MTTF_D$ of 20 years is assumed to be given by the manufacturer. Applying the parts count method of D.1, to calculate the $MTTF_{D,C2}$ of the second channel gives

$$\frac{1}{MTTF_{D,C2}} = \frac{1}{MTTF_{D,SW2}} + \frac{1}{MTTF_{D,PLC}} + \frac{1}{MTTF_{D,CC}} = \frac{1}{139 \text{ years}} + \frac{1}{20 \text{ years}} + \frac{1}{20 \text{ years}} = \frac{0,1072}{\text{year}} \quad (I.3)$$

which gives an $MTTF_D = 9,3$ years for the channel, which is “low” according to 6.1.4, Table 6.

NOTE If no $MTTF_D$ information for SW1B, SW2 or K1B is available, a worst-case assumption according to C.2 or C.4 can be made.

As both channels have different values of $MTTF_D$, Formula (D.2) can be used to calculate equivalent identical values of $MTTF_D$ for a symmetrical two-channel system. Applying this formula yields an $MTTF_D = 37$ years for each channel, which is “high” according to 6.1.4, Table 6.

— T_{10D}

The method of C.4.2 gives $T_{10D,SW1B}$ of 278 years, $T_{10D,K1B}$ of 5.5 years and $T_{10D,SW2}$ of 13,9 years, with the latter two being lower than the mission time of 20 years. The estimation of PL and PFH is therefore only valid if K1B is exchanged before 5,5 years and if SW2 is exchanged before 13,9 years of operation respectively.

— DC

In control circuit B, five of the SRP/CS are tested by the PLC. This testing consists of SW1B, SW2 and K1B being read back by the PLC, the CC being read back by the PLC via RS and the PLC performing self-tests. The DC values associated with each of these tested parts are

- $DC_{SW1B} = DC_{SW2} = 99 \%$, “high”, due to plausibility check, see Table E.1 (second line of input device part),
- $DC_{K1B} = 99 \%$, “high”, due to normally open and normally closed mechanically linked contacts, see Table E.1 (second line of input device part),
- $DC_{PLC} = 30 \%$, “none” due to low effectiveness of self-tests (this value comes out of the specific application), and
- $DC_{CC} = 90 \%$, “medium”, due to indirect monitoring of the machine actuator by control logic, see Table E.1 (sixth line of output device part) – if the PLC monitors a failure of CC, it is able to stop the motion with the enable (standard) and to de-energize the contactor relay K1B (additional shut-off path).

For an estimation of the PL, an average DC value is needed as input for Figure 12:

$$DC_{avg} = \frac{\frac{DC_{SW1B}}{MTTF_{D,SW1B}} + \frac{DC_{K1B}}{MTTF_{D,K1B}} + \frac{DC_{SW2}}{MTTF_{D,SW2}} + \frac{DC_{PLC}}{MTTF_{D,PLC}} + \frac{DC_{CC}}{MTTF_{D,CC}}}{\frac{1}{MTTF_{D,SW1B}} + \frac{1}{MTTF_{D,K1B}} + \frac{1}{MTTF_{D,SW2}} + \frac{1}{MTTF_{D,PLC}} + \frac{1}{MTTF_{D,CC}}} = \frac{\frac{0,99}{2778} + \frac{0,99}{56} + \frac{0,99}{139} + \frac{0,3}{20} + \frac{0,9}{20}}{\frac{1}{2778} + \frac{1}{56} + \frac{1}{139} + \frac{1}{20} + \frac{1}{20}} = \frac{0,09}{0,13} = 67,9 \quad (I.4)$$

Thus, the resulting DC_{avg} is “low”.

— CCF

For an estimation of the measures against CCF according to [F.2](#), the scores for control circuit B are given in [Table I.1](#).

Table I.1 — Estimation of the measures against CCF for example B

No.	Item	Implemented measures	Score for control circuit	Maximum possible score
1	Separation/segregation			
	physical separation between signal paths	— separate wiring to PLC between SW1B and SW2 (signal cables routed separately) — separation of both functional channels in the cabinet, e.g. between K1B and CC (separate components) — cross-connection of both channels limited to diagnostic testing	15	15
2	Diversity			
	different technologies/design or physical principles are used	— position switch SW1B is operated when the safety guard is opened and has a break-contact element with direct opening action while position switch SW2 is operated when the safety guard is closed and uses a make-contact element. — one functional channel uses electromechanical components, the other programmable electronic components	20	20
3	Design/application/experience			
3.1	protection against over-voltage, over-pressure, over-current, over-temperature.	— additional protection against over-voltage and over-current on system level using external protection components where needed, i.e. diodes, fuses on inputs and outputs and a free-wheeling diode on relay K1B — over-voltage and under-voltage detection in the PLC	15	15
3.2	components used are well-tried	Only switch SW1B and relay K1B are well-tried components	none (only partly fulfilled, see F.2)	5
4	Assessment/analysis			
	For each part of SRP/CS a failure mode and effect analysis has been carried out and its results taken into account to avoid common-cause-failures in the design.	not completely implemented (FMEA with focus on CCF has been carried out but not in a formalized and completely documented way)	None	5
5	Training			
	Training of designers to understand the causes and consequences of CCFs.	not completely implemented	None	5
6	Environmental			

Table I.1 (continued)

No.	Item	Implemented measures	Score for control circuit	Maximum possible score
6.1	For electrical/electronic systems, prevention of contamination and EMIs to protect against CCFs in accordance with appropriate standards (e.g. IEC 61326-3-1).	— additional protection against electromagnetic disturbances on system level using external protection components, as diodes, fuses, filters and shielding on all inputs and outputs (appropriate measures of Table L.1 implemented with focus on CCF) — signal and power cables are routed separately	25	25
6.2	Other Influences Consideration of the requirements for immunity to all relevant environmental influences such as, temperature, shock, vibration, humidity (e.g. as specified in relevant standards).	— choice of both position switches to withstand all expected environmental influences with sufficient overdimensioning and consideration of possible CCF causes. — K1B, PLC and CC installed in the cabinet with temperature control	10	10
	Total		85	Max. 100

Sufficient measures against CCF require a minimum score of 65, so for example B the score of 85 is sufficient to fulfil the requirements against CCF.

The characteristics of category 3 are fulfilled because a single fault in any of the parts does not lead to the loss of the safety function. Whenever reasonably practicable the single fault is detected at or before the next demand upon the safety function, the average diagnostic coverage (DC_{avg}) is in the range 60 % to 90 %, the measures against CCF are sufficient and the equivalent $MTTF_D$ for each channel is “high”.

Input data for [Figure 12](#): $MTTF_D$ for the channel is “high” (37 years), DC_{avg} is “low” and category is 3.

Using [Figure 12](#) this can be interpreted as performance level d.

Application of [Annex K](#) (use 36 years) gives an PFH of $5,16 \times 10^{-7}/h$ and PL d.

This result matches the PL_{rd} according to [1.2](#). Control circuit B therefore satisfies the requirements for risk reduction of the example B application of [1.2](#) with S2, F2, P1 and PL_{rd} .

Annex J
(informative)

Example of SRESW realisation

J.1 Description of example

In this annex the process steps for realizing the SRESW of an SRP/CS for PL_r d are presented. The SRP/CS is interfaced with the machine equipment. It ensures

- the acquisition of information sent by the various sensors,
- the processing required to operate the power control elements taking into account the safety requirements, and
- the piloting of the power control elements.

The function diagram of this application’s SRESW is as shown in [Figure J.1](#).

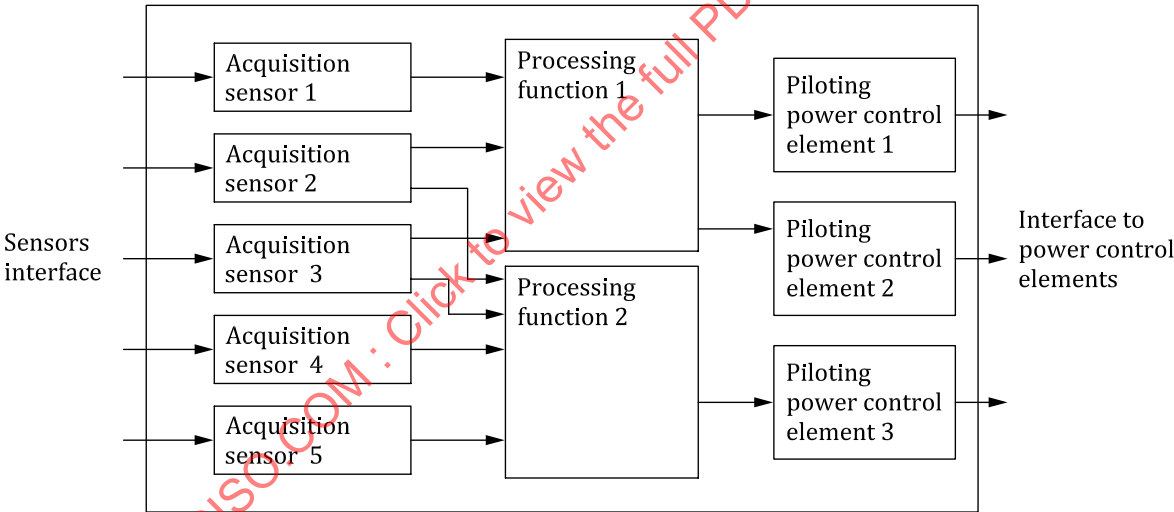


Figure J.1 — Function block level design of software example

J.2 Application of V-model of software safety lifecycle

[Table J.1](#) presents the development activities, their corresponding verification steps, and the related documentation. These activities follow the V-model of software safety lifecycle according to [Figure 14 a](#)).

Table J.1 — Activities and documents within software safety lifecycle

Development activity	Lifecycle activity	Associated documentation
machine aspect (hardware and software): identification of the functions involving the SRP/CS	— identification of safety functions	Output: — safety requirements specification (SRS)
architecture aspect (hardware and software): definition of the control architecture with sensors and power control elements	— comments upon safety characteristics of chosen components — planning of the test of the SRS	Output: — definition of the control architecture — test plan for SRS
software specification aspect: — specification of the requirements of the safety-related software (SRSS), including — transcription of machine functions into software functions	— review of the descriptions SRSS against SRS (see L.3) — planning of the test of the SRSS against the SRS	Input: — safety requirements specification (SRS) Output: — software design specification (SDS) including software descriptions — test plan for the SDS — documentation of review activity
software architecture aspect: — software system design, including to detail the functions into functional blocks	— review of the system design against the SDS including definition of critical blocks which are subject of greater review and validation effort — planning of the test of the software system design	Input: — SDS Output: — software system design specification (SSDS) including function block modelling — test plan for the SSDS — documentation of review activity
design of the software modules	— review of the software module design against the SSDS. — planning of the test of the software modules	Input: — SSDS Output: — module design specification (MDS) — test plan for the MDS — documentation of review activity
coding aspect: coding of non-existing software modules according to the programming rules (see L.4)	— review of the code against the MDS — verification of functions and compliance with rules	Input: — MDS Output: — reviewed code including Encoding comments in the code — documentation of review activity
NOTE Each test plan contains: — a correspondence matrix which cross-references specification paragraphs and tests; — test sheets comprising test scenario and comments upon results achieved.		

Table J.1 (continued)

Development activity	Lifecycle activity	Associated documentation
validation aspect: — module test	test of the software modules against the MDS according to the test plan for the MDS including — verification of the test coverage — verification of the test results	Input: — reviewed code — MDS — test plan for the MDS Output: — tested software modules — documentation of test activity
validation aspect: — software integration testing	test of the integrated software against the SSDS according to the test plan for the SSDS including — verification of the test coverage — verification of the test results The test may include the final hardware (if possible).	Input: — tested software modules — SSDS — test plan for the MDS Output: — tested integration — documentation of test activity
validation aspect: — validation of the SRP/CS making of test scenarios: — operation aspect of functions — behaviour-on-failure aspect	test of the integrated software and hardware (the SRP/CS) against the SDS according to the test plan for the SDS including — verification of the test coverage — verification of the test results The test may include the final hardware (if possible).	Input: — SDS — test plan for the SDS Output: — validated software (of the SRP/CS) — documentation of test activity
NOTE Each test plan contains: — a correspondence matrix which cross-references specification paragraphs and tests; — test sheets comprising test scenario and comments upon results achieved.		

J.3 Verification of software specification at different levels (i.e. SDS, SSDS, MDS)

As part of the software safety lifecycle according to [Figure 14 a\)](#), the verification activities at each level of the software specifications consists in reading the specifications in order to verify that all the sensitive points are properly described. The following should be considered when verifying each software function:

- limiting the cases of erroneous interpretation of the software specifications;
- avoiding gaps in the specifications resulting in an unknown behaviour of the SRP/CS;
- precisely defining conditions for activation and de-activation of functions;
- precisely guaranteeing that all the possible cases are handled;
- consistency tests;
- the different parameterizing cases;
- the reaction following a failure.

J.4 Example of programming rules

In general, it should be possible to identify the software version. Modifications should be documented with author, date and type of modification. Concerning the programming rules the following rules can be differentiated.

a) Programming rules at the program structure level

The programming should be structured in order to display a consistent and understandable general skeleton allowing the different processing to be easily localized. This implies

- 1) the use of templates for typical program or function blocks,
- 2) partitioning of the program into segments in order to identify main parts corresponding to "inputs", "processing" and "outputs",
- 3) comments should appear on each program section in the source of the program to facilitate the updating of the comment in case of modification,
- 4) the description of the role a function block has when calling this block,
- 5) that memory location should be used only by one single kind of data type and be marked by unique labels, and
- 6) that the working sequence should not depend on variables such as a jump address calculated at runtime of the program, conditional jumps being authorized.

b) Programming rules regarding the use of variables

- 1) The activation or de-activation of any output should take place only once (centralized conditions).
- 2) The program should be structured such that the equations for updating a variable are centralized.
- 3) Each global variable, input or output should have a mnemonic name explicit enough and be described by a comment within the source.

c) Programming rules at the function block level

- 1) Function blocks that have been validated by the supplier of the SRP/CS should be used. It should be checked that the assumed operating conditions for these validated blocks correspond to the conditions of the program.
- 2) The size of the coded block should be limited to the following guideline values:
 - parameters: maximum eight digital and two integer inputs, four outputs;
 - in function code: maximum 10 local variables, maximum 20 Boolean equations.
- 3) The function blocks should not modify the global variables.
- 4) Each value should be compared to expected pre-set benchmarks to ensure its validity.
- 5) The input parameters of a function block should be checked for inconsistencies.
- 6) Each fault code should be accessible and allow a clear identification of the original fault.
- 7) The fault codes and the state of the block after fault detection should be described by comments.
- 8) The resetting of the block or the restoration of a normal state should be described by comments.

Annex K
(informative)

Numerical representation of [Figure 12](#)

STANDARDSISO.COM : Click to view the full PDF of ISO 13849-1:2023

Table K.1 — Numerical representation of Figure 12

MTTF _D for each channel years	Average frequency of a dangerous failure per hour (PFH) (1/h) and corresponding performance level							
	Cat. B DC _{avg} = none	Cat. 1 DC _{avg} = none	Cat. 2 DC _{avg} = low	Cat. 2 DC _{avg} = medium	Cat. 3 DC _{avg} = low	Cat. 3 DC _{avg} = medium	Cat. 4 DC _{avg} = high	
3	3,80 × 10 ⁻⁵	a	2,58 × 10 ⁻⁵	a	1,99 × 10 ⁻⁵	a	6,09 × 10 ⁻⁶	b
3,3	3,46 × 10 ⁻⁵	a	2,33 × 10 ⁻⁵	a	1,79 × 10 ⁻⁵	a	5,41 × 10 ⁻⁶	b
3,6	3,17 × 10 ⁻⁵	a	2,13 × 10 ⁻⁵	a	1,62 × 10 ⁻⁵	a	4,86 × 10 ⁻⁶	b
3,9	2,93 × 10 ⁻⁵	a	1,95 × 10 ⁻⁵	a	1,48 × 10 ⁻⁵	a	4,40 × 10 ⁻⁶	b
4,3	2,65 × 10 ⁻⁵	a	1,76 × 10 ⁻⁵	a	1,33 × 10 ⁻⁵	a	3,89 × 10 ⁻⁶	b
4,7	2,43 × 10 ⁻⁵	a	1,60 × 10 ⁻⁵	a	1,20 × 10 ⁻⁵	a	3,48 × 10 ⁻⁶	b
5,1	2,24 × 10 ⁻⁵	a	1,47 × 10 ⁻⁵	a	1,10 × 10 ⁻⁵	a	3,15 × 10 ⁻⁶	b
5,6	2,04 × 10 ⁻⁵	a	1,33 × 10 ⁻⁵	a	9,87 × 10 ⁻⁶	b	2,80 × 10 ⁻⁶	c
6,2	1,84 × 10 ⁻⁵	a	1,19 × 10 ⁻⁵	a	8,80 × 10 ⁻⁶	b	2,47 × 10 ⁻⁶	c
6,8	1,68 × 10 ⁻⁵	a	1,08 × 10 ⁻⁵	a	7,93 × 10 ⁻⁶	b	2,20 × 10 ⁻⁶	c
7,5	1,52 × 10 ⁻⁵	a	9,75 × 10 ⁻⁶	b	7,10 × 10 ⁻⁶	b	1,95 × 10 ⁻⁶	c
8,2	1,39 × 10 ⁻⁵	a	8,87 × 10 ⁻⁶	b	6,43 × 10 ⁻⁶	b	1,74 × 10 ⁻⁶	c
9,1	1,25 × 10 ⁻⁵	a	7,94 × 10 ⁻⁶	b	5,74 × 10 ⁻⁶	b	1,53 × 10 ⁻⁶	c
10	1,14 × 10 ⁻⁵	a	7,18 × 10 ⁻⁶	b	5,14 × 10 ⁻⁶	b	1,36 × 10 ⁻⁶	c
11	1,04 × 10 ⁻⁵	a	6,44 × 10 ⁻⁶	b	4,53 × 10 ⁻⁶	b	1,18 × 10 ⁻⁶	c
12	9,51 × 10 ⁻⁶	b	5,84 × 10 ⁻⁶	b	4,04 × 10 ⁻⁶	b	1,04 × 10 ⁻⁶	c
13	8,78 × 10 ⁻⁶	b	5,33 × 10 ⁻⁶	b	3,64 × 10 ⁻⁶	b	9,21 × 10 ⁻⁷	d
15	7,61 × 10 ⁻⁶	b	4,53 × 10 ⁻⁶	b	3,01 × 10 ⁻⁶	b	7,44 × 10 ⁻⁷	d
16	7,13 × 10 ⁻⁶	b	4,21 × 10 ⁻⁶	b	2,77 × 10 ⁻⁶	c	6,76 × 10 ⁻⁷	d
18	6,34 × 10 ⁻⁶	b	3,68 × 10 ⁻⁶	b	2,37 × 10 ⁻⁶	c	5,67 × 10 ⁻⁷	d
20	5,71 × 10 ⁻⁶	b	3,26 × 10 ⁻⁶	b	2,06 × 10 ⁻⁶	c	4,85 × 10 ⁻⁷	d
22	5,19 × 10 ⁻⁶	b	2,93 × 10 ⁻⁶	c	1,82 × 10 ⁻⁶	c	4,21 × 10 ⁻⁷	d

NOTE 1 If for category 2 the demand rate is less than or equal to 1/25 of the test rate (see 6.1.3.2.4), then the PFH values stated in this table for category 2 multiplied by a factor of 1,1 can be used as a worst-case estimate.

NOTE 2 The calculation of the PFH values was based on the following DC_{avg}:

- DC_{avg} = low, calculated with 60 %;
- DC_{avg} = medium, calculated with 90 %;
- DC_{avg} = high, calculated with 99 %.

Table K.1 (continued)

Average frequency of a dangerous failure per hour (PFH) (1/h) and corresponding performance level								
MTTF _D for each channel years	Cat. B	Cat. 1	Cat. 2	Cat. 2	Cat. 3	Cat. 3	Cat. 4	
	DC _{avg} = none	DC _{avg} = none	DC _{avg} = low	DC _{avg} = medium	DC _{avg} = low	DC _{avg} = medium	DC _{avg} = high	
24	4,76 × 10 ⁻⁶	b	2,65 × 10 ⁻⁶	c	1,62 × 10 ⁻⁶	c	3,70 × 10 ⁻⁷	d
27	4,23 × 10 ⁻⁶	b	2,32 × 10 ⁻⁶	c	1,39 × 10 ⁻⁶	c	8,04 × 10 ⁻⁷	d
30			3,80 × 10 ⁻⁶	b	2,06 × 10 ⁻⁶	c	1,21 × 10 ⁻⁶	c
33			3,46 × 10 ⁻⁶	b	1,85 × 10 ⁻⁶	c	1,06 × 10 ⁻⁶	c
36			3,17 × 10 ⁻⁶	b	1,67 × 10 ⁻⁶	c	9,39 × 10 ⁻⁷	d
39			2,93 × 10 ⁻⁶	c	1,53 × 10 ⁻⁶	c	8,40 × 10 ⁻⁷	d
43			2,65 × 10 ⁻⁶	c	1,37 × 10 ⁻⁶	c	7,34 × 10 ⁻⁷	d
47			2,43 × 10 ⁻⁶	c	1,24 × 10 ⁻⁶	c	6,49 × 10 ⁻⁷	d
51			2,24 × 10 ⁻⁶	c	1,13 × 10 ⁻⁶	c	5,80 × 10 ⁻⁷	d
56			2,04 × 10 ⁻⁶	c	1,02 × 10 ⁻⁶	c	5,10 × 10 ⁻⁷	d
62			1,84 × 10 ⁻⁶	c	9,06 × 10 ⁻⁷	d	4,43 × 10 ⁻⁷	d
68			1,68 × 10 ⁻⁶	c	8,17 × 10 ⁻⁷	d	3,90 × 10 ⁻⁷	d
75			1,52 × 10 ⁻⁶	c	7,31 × 10 ⁻⁷	d	3,40 × 10 ⁻⁷	d
82			1,39 × 10 ⁻⁶	c	6,61 × 10 ⁻⁷	d	3,01 × 10 ⁻⁷	d
91			1,25 × 10 ⁻⁶	c	5,88 × 10 ⁻⁷	d	2,61 × 10 ⁻⁷	d
100			1,14 × 10 ⁻⁶	c	5,28 × 10 ⁻⁷	d	2,29 × 10 ⁻⁷	d
110							1,01 × 10 ⁻⁷	d
120								e
130								e
150								e
160								e
180								e

NOTE 1 If for category 2 the demand rate is less than or equal to 1/25 of the test rate (see 6.1.3.2.4), then the PFH values stated in this table for category 2 multiplied by a factor of 1,1 can be used as a worst-case estimate.

NOTE 2 The calculation of the PFH values was based on the following DC_{avg}:

- DC_{avg} = low, calculated with 60 %;
- DC_{avg} = medium, calculated with 90 %;
- DC_{avg} = high, calculated with 99 %.

NOTE 1 If for category 2 the demand rate is less than or equal to 1/25 of the test rate (see 6.1.3.2.4), then the PFH values stated in this table for category 2 multiplied by a factor of 1,1 can be used as a worst-case estimate.

NOTE 2 The calculation of the PFH values was based on the following DC_{avg}:

- DC_{avg} = low, calculated with 60 %;
- DC_{avg} = medium, calculated with 90 %;
- DC_{avg} = high, calculated with 99 %.

Table K.1 (continued)

MTTF _D for each channel years	Average frequency of a dangerous failure per hour (PFH) (1/h) and corresponding performance level					
	Cat. B DC _{avg} = none	Cat. 1 DC _{avg} = none	Cat. 2 DC _{avg} = low	Cat. 2 DC _{avg} = medium	Cat. 3 DC _{avg} = low	Cat. 3 DC _{avg} = medium
200						DC _{avg} = high 1,19 × 10 ⁻⁸ e
220						1,08 × 10 ⁻⁸ e
240						9,81 × 10 ⁻⁹ e
270						8,67 × 10 ⁻⁹ e
300						7,76 × 10 ⁻⁹ e
330						7,04 × 10 ⁻⁹ e
360						6,44 × 10 ⁻⁹ e
390						5,94 × 10 ⁻⁹ e
430						5,38 × 10 ⁻⁹ e
470						4,91 × 10 ⁻⁹ e
510						4,52 × 10 ⁻⁹ e
560						4,11 × 10 ⁻⁹ e
620						3,70 × 10 ⁻⁹ e
680						3,37 × 10 ⁻⁹ e
750						3,05 × 10 ⁻⁹ e
820						2,79 × 10 ⁻⁹ e
910						2,51 × 10 ⁻⁹ e
1 000						2,28 × 10 ⁻⁹ e
1 100						2,07 × 10 ⁻⁹ e
1 200						1,90 × 10 ⁻⁹ e
1 300						1,75 × 10 ⁻⁹ e
1 500						1,51 × 10 ⁻⁹ e

NOTE 1 If for category 2 the demand rate is less than or equal to 1/25 of the test rate (see 6.1.3.2.4), then the PFH values stated in this table for category 2 multiplied by a factor of 1,1 can be used as a worst-case estimate.

NOTE 2 The calculation of the PFH values was based on the following DC_{avg}:

- DC_{avg} = low, calculated with 60 %;
- DC_{avg} = medium, calculated with 90 %;
- DC_{avg} = high, calculated with 99 %.

Table K.1 (continued)

MTTF _D for each channel	Average frequency of a dangerous failure per hour (PFH) (1/h) and corresponding performance level					
	Cat. B DC _{avg} = none	Cat. 1 DC _{avg} = none	Cat. 2 DC _{avg} = low	Cat. 2 DC _{avg} = medium	Cat. 3 DC _{avg} = low	Cat. 3 DC _{avg} = medium
years						
1 600						1,42 × 10 ⁻⁹ e
1 800						1,26 × 10 ⁻⁹ e
2 000						1,13 × 10 ⁻⁹ e
2 200						1,03 × 10 ⁻⁹ e
2 300						9,85 × 10 ⁻¹⁰ e
2 400						9,44 × 10 ⁻¹⁰ e
2 500						9,06 × 10 ⁻¹⁰ e
NOTE 1 If for category 2 the demand rate is less than or equal to 1/25 of the test rate (see 6.1.3.2.4), then the PFH values stated in this table for category 2 multiplied by a factor of 1,1 can be used as a worst-case estimate.						
NOTE 2 The calculation of the PFH values was based on the following DC _{avg} :						
— DC _{avg} = low, calculated with 60 %;						
— DC _{avg} = medium, calculated with 90 %;						
— DC _{avg} = high, calculated with 99 %.						

Annex L (informative)

Electromagnetic interference (EMI) immunity

The following routes (see Figure L.1) provide guidance to fulfil EMI immunity measures for an SRP/CS or subsystems.

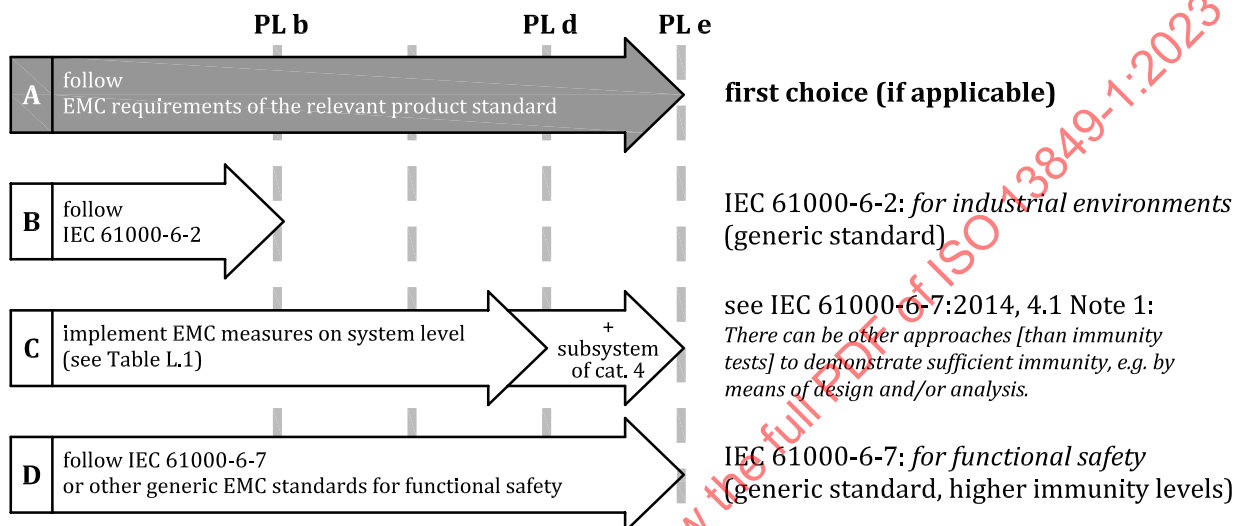


Figure L.1 — Route to fulfil EMI measures

At least one or more routes should be selected and fully applied:

- Route A: follow the EMI requirements of the relevant product standard (see IEC 61000-6-7:2014, 4.1, 1st sentence). An example of a product standard is IEC 61800-5-2;
- Route B: for PL_r a and b, follow the EMI requirements of IEC 61000-6-2;
- Route C: for any PL_r, implement EMI measures to achieve a score of at least 280 (of possible 390) for dual channel subsystem (Cat 2, Cat 3 and Cat 4) and 230 for single channel subsystem (Cat B and Cat 1) according to Table L.1 (see IEC 61000-6-7:2014, 4.1, Note 1); for PL_r e, this route can only be applied if the requirements of category 4 are additionally fulfilled;
- Route D: follow generic EMI standards for functional safety as IEC 61000-6-7 or IEC 61326-3-1.

For electromechanical components with integrated active electronics, the effect of EMI on the execution of the safety functions should be analysed and the relevant measures to achieve EMI should be implemented. If route C is selected, the measures listed in [Table L.1](#) should be evaluated according to their effectiveness to avoid or control EMI effects. Engineering judgement should prove (e.g. using FMEA techniques) that those typical causes for EMI are reduced as much as reasonably possible. The selected routes/measures should be clearly documented with adequate proof of compliance to the selected route.

Where tests are applied for validation, they should ensure that the safety function is exercised and exposed to the EMI immunity for an adequate duration to demonstrate no susceptibilities are present.

Table L.1 — Measures to achieve EMI immunity for an SRP/CS or subsystem(s)

Measures to achieve EMI	Score ^a
Safety-related sensors and their wire harness	
application of the measures described in IEC 60204-1:2016+AMD1:2021, Annex H and/or IEC 61800-3 (hr)	10
analog voltage signals, angle encoder shielded and either grounded or twisted cables, or both, for sensors and safety-related input/output-signals (cable shields are contacted all-around and flat contacted in low impedance close to the components) (hr)	20
harnesses and wiring of low voltage DC between components is in twisted pair cabling	10
Safety-related IO system (central or decentral or integrated in the PLC)	
installed in a shielded and bonded cabinet or components in a shielded and bonded housing (hr)	20
Control system and/or specific components are divided into zones ^b , e.g. a) mains supply and power distribution; b) strong interferers, e.g. mains filter, mains chokes, heating components, high power supplies and motor cables; c) sensitive components e.g. low voltage power supplies, PLCs, data busses, sensors and low voltage actuators. (hr)	20
PLC as part of SRP/CS	
installed in a shielded and bonded cabinet or components in a shielded and bonded housing	10
category 3/4 for PL _r d/e with diverse PLC in the same enclosure separated with sufficient distance in accordance with the manufacture installation instruction	10 ^{c, d}
category 3/4 for PL _r d/e with redundant PLC in different enclosures	20 ^{c, d}
category 3/4 for PL _r d/e with diverse channels (e.g. PLC and discrete logic) or using safety PLC	20 ^{c, d}
Safety-related actuator and their wire harness	
application of the measures described in IEC 60204-1:2016+AMD1:2021, Annex H and/or usage of IEC 61800-3(hr)	10
Other components and wiring with relevant disturbance level	
shielded and bonded cables for motors or sinewave filter between motor and inverter or equivalent measures in accordance with the manufacture installation instruction where applicable (hr)	20
RF-filter, overvoltage and transient protection (e.g. filter, transient-voltage suppression diode, optocoupler, ferrites) for safety-related input signals in accordance with the manufacture installation instruction where applicable (hr)	20
EMI filters (as per manufacturers installation instructions or specifically intended for the application) for power mains (e.g. overvoltage and transient protection)	20
application of the measures described in IEC 60204-1:2016+AMD1:2021, Annex H and/or usage of IEC 61800-3	10
Engineering, programming, training, field observation	
all components fulfil at minimum the requirements against EMI generic standards IEC 61000-6-2 (mentioned in manufacturers documentation) (hr)	30
risk analysis for EMI (see example in Table L.2) and risk assessment with a final report	20
diverse redundant channels (see NOTE)	20 ^c