INTERNATIONAL STANDARD

ISO 13849-1

Third edition
2015-12-15

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

Part 1: General principles for design

Sécurité des machines — Parties des systèmes de commande relatives à la sécurité —

Partie 1: Principes généraux de conception

Reference number
ISO 13849-1:2015(E)

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

Contents

Page

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 on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

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

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

— deletion of the former Table 1 from the Introduction,

— updating and addition of normative references,

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

— addition of a new term and definition, *proven in use*,

— editorial, but not technical, modification of Figure 1,

— a new subclause, 4.5.5, as well as modifications to existing sections including the annexes, substantial modification of Annex C and an entirely new Annex I.

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

— *Part 1: General principles for design*

— *Part 2: Validation*

Introduction

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

a) Type-A standards (basis standards) give basic concepts, principles for design and general aspects that can be applied to machinery.

b) Type-B standards (generic safety standards) deal with one or more safety aspect(s), or one or more type(s) of safeguards that can be used across a wide range of machinery:

   — type-B1 standards on particular safety aspects (e.g. safety distances, surface temperature, noise);

   — type-B2 standards on safeguards (e.g. two-hands controls, interlocking devices, pressure sensitive devices, guards).

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

This part of ISO 13849 is a type-B-1 standard as stated in ISO 12100.

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

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

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

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

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

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

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

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

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

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

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

For machines which are covered by the scope of a type-C standard and which have been designed and built according to the requirements of that standard, the requirements of that type-C standard take precedence.

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

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

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

Parts of machinery control systems that are assigned to provide safety functions are called safety-related parts of control systems (SRP/CS) and these can consist of hardware and software and can either be separate from the machine control system or an integral part of it. In addition to providing safety functions, SRP/CS can also provide operational functions (e.g. two-handed controls as a means of process initiation).

The ability of safety-related parts of control systems to perform a safety function under foreseeable conditions is allocated one of five levels, called performance levels (PL). These performance levels are defined in terms of probability of dangerous failure per hour (see Table 2).

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

In order to assist the designer and facilitate the assessment of achieved PL, this document employs a methodology based on the categorization of structures according to specific design criteria and specified behaviours under fault conditions. These categories are allocated one of five levels, termed Categories B, 1, 2, 3 and 4.

The performance levels and categories can be applied to safety-related parts of control systems, such as

— protective devices (e.g. two-hand control devices, interlocking devices), electro-sensitive protective devices (e.g. photoelectric barriers), pressure sensitive devices,

— control units (e.g. a logic unit for control functions, data processing, monitoring, etc.), and

— power control elements (e.g. relays, valves, etc.),

as well as to control systems carrying out safety functions at all kinds of machinery — from simple (e.g. small kitchen machines, or automatic doors and gates) to manufacturing installations (e.g. packaging machines, printing machines, presses).

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

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

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

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

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

Part 1: General principles for design

1 Scope

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

It does not specify the safety functions or performance levels that are to be used in a particular case.

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

It does not give specific requirements for the design of products which are parts of SRP/CS. Nevertheless, the principles given, such as categories or performance levels, can be used.

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

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

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

NOTE 4 For safety-related embedded software for components with PL_r = e, see IEC 61508–3:1998, Clause 7.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 12100:2010, *Safety of machinery — General principles for design — Risk assessment and risk reduction*

ISO 13849-2:2012, *Safety of machinery — Safety-related parts of control systems — Part 2: Validation*

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

IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements.* Corrected by IEC 61508-3/Cor.1:1999

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

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

ISO/TR 22100-2:2013, *Safety of machinery — Relationship with ISO 12100 — Part 2: How ISO 12100 relates to ISO 13849-1*

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

3 Terms, definitions, symbols and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 12100 and IEC 60050-191 and the following apply.

3.1.1
safety–related part of a control system
SRP/CS
part of a control system that responds to safety-related input signals and generates safety-related output signals

Note 1 to entry: The combined safety-related parts of a control system start at the point where the safety-related input signals are initiated (including, for example, the actuating cam and the roller of the position switch) and end at the output of the power control elements (including, for example, the main contacts of a contactor).

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

3.1.2
category
classification of the safety-related parts of a control system in respect of their resistance to faults and their subsequent behaviour in the fault condition, and which is achieved by the structural arrangement of the parts, fault detection and/or by their reliability

3.1.3
fault
state of an item characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources

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

Note 2 to entry: In this part of ISO 13849, "fault" means *random fault*.

[SOURCE: IEC 60050-191:1990, 05-01.]

3.1.4
failure
termination of the ability of an item to perform a required function

Note 1 to entry: After a failure, the item has a fault.

Note 2 to entry: "Failure" is an event, as distinguished from "fault", which is a state.

Note 3 to entry: The concept as defined does not apply to items consisting of software only.

Note 4 to entry: Failures which only affect the availability of the process under control are outside of the scope of this part of ISO 13849.

[SOURCE: IEC 60050–191:1990, 04-01.]

3.1.5
dangerous failure
failure which has the potential to put the SRP/CS in a hazardous or fail-to-function state

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

Note 2 to entry: [SOURCE: IEC 61508–4, 3.6.7, modified.]

3.1.6
common cause failure
CCF
failures of different items, resulting from a single event, where these failures are not consequences of each other

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

[SOURCE: IEC 60050-191-am1:1999, 04-23.]

3.1.7
systematic failure
failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

Note 1 to entry: Corrective maintenance without modification will usually not eliminate the failure cause.

Note 2 to entry: A systematic failure can be induced by simulating the failure cause.

Note 3 to entry: Examples of causes of systematic failures include human error in

— the safety requirements specification,

— the design, manufacture, installation, operation of the hardware, and

— the design, implementation, etc., of the software.

[SOURCE: IEC 60050-191:1990, 04-19.]

3.1.8
muting
temporary automatic suspension of a safety function(s) by the SRP/CS

3.1.9
manual reset
function within the SRP/CS used to restore manually one or more safety functions before re-starting a machine

3.1.10
harm
physical injury or damage to health

[SOURCE: ISO 12100:2010, 3.5.]

3.1.11
hazard
potential source of harm

Note 1 to entry: A hazard can be qualified in order to define its origin (e.g. mechanical hazard, electrical hazard) or the nature of the potential harm (e.g. electric shock hazard, cutting hazard, toxic hazard, 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 may 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.]

3.1.12
hazardous situation
circumstance in which a person is exposed to at least one hazard

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

[SOURCE: ISO 12100:2010, 3.10.]

3.1.13
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO 12100:2010, 3.12.]

3.1.14
residual risk
risk remaining after protective measures have been taken

Note 1 to entry: See Figure 2.

[SOURCE: ISO 12100:2010, 3.13, modified.]

3.1.15
risk assessment
overall process comprising risk analysis and risk evaluation

[SOURCE: ISO 12100:2010, 3.17.]

3.1.16
risk analysis
combination of the specification of the limits of the machine, hazard identification and risk estimation

[SOURCE: ISO 12100:2010, 3.15.]

3.1.17
risk evaluation
judgement, on the basis of risk analysis, of whether risk reduction objectives have been achieved

[SOURCE: ISO 12100:2010, 3.16.]

3.1.18
intended use of a machine
use of the machine in accordance with the information provided in the instructions for use

[SOURCE: ISO 12100:2010, 3.23.]

3.1.19
reasonably foreseeable misuse
use of a machine in a way not intended by the designer, but which may result from readily predictable human behaviour

[SOURCE: ISO 12100:2010, 3.24.]

3.1.20
safety function
function of the machine whose failure can result in an immediate increase of the risk(s)

[SOURCE: ISO 12100:2010, 3.30.]

3.1.21
monitoring
safety function which ensures that a protective measure is initiated if the ability of a component or an element to perform its function is diminished or if the process conditions are changed in such a way that a decrease of the amount of risk reduction is generated

3.1.22
programmable electronic system
PES
system for control, protection or monitoring dependent for its operation on one or more programmable electronic devices, including all elements of the system such as power supplies, sensors and other input devices, contactors and other output devices

[SOURCE: IEC 61508-4:1998, 3.3.2, modified.]

3.1.23
performance level
PL
discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions

Note 1 to entry: See 4.5.1.

3.1.24
required performance level
PL_r
performance level (PL) applied in order to achieve the required risk reduction for each safety function

Note 1 to entry: See Figures 2 and A.1.

3.1.25
mean time to dangerous failure
$MTTF_D$
expectation of the mean time to dangerous failure

[SOURCE: IEC 62061:2005, 3.2.34, modified.]

3.1.26
diagnostic coverage
DC
measure of the effectiveness of diagnostics, which may be determined as the ratio between the failure rate of detected dangerous failures and the failure rate of total dangerous failures

Note 1 to entry: Diagnostic coverage can exist for the whole or parts of a safety-related system. For example, diagnostic coverage could exist for sensors and/or logic system and/or final elements.

[SOURCE: IEC 61508-4:1998, 3.8.6, modified.]

3.1.27
protective measure
measure intended to achieve risk reduction

EXAMPLE 1 Implemented by the designer: inherent design, safeguarding and complementary protective measures, information for use.

EXAMPLE 2 Implemented by the user: organization (safe working procedures, supervision, permit-to-work systems), provision and use of additional safeguards, personal protective equipment, training.

[SOURCE: ISO 12100:2010, 3.19, modified.]

3.1.28
mission time
T_M
period of time covering the intended use of an SRP/CS

3.1.29
test rate
r_t
frequency of automatic tests to detect faults in a SRP/CS, reciprocal value of diagnostic test interval

3.1.30
demand rate
r_D
frequency of demands for a safety-related action of the SRP/CS

3.1.31
repair rate
r_r
reciprocal value of the period of time between detection of a dangerous failure by either an online test or obvious malfunction of the system and the restart of operation after repair or system/component replacement

Note 1 to entry: The repair time does not include the span of time needed for failure-detection.

3.1.32
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, mechanical).

3.1.33
safety integrity level
SIL
discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

[SOURCE: IEC 61508-4:1998, 3.5.6.]

3.1.34
limited variability language
LVL
type of language that provides the capability of combining predefined, application-specific library functions to implement the safety requirements specifications

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

Note 2 to entry: A typical example of a system using LVL: PLC.

[SOURCE: IEC 61511-1:2003, 3.2.80.1.2, modified.]

3.1.35
full variability language
FVL
type of language that provides the capability of implementing a wide variety of functions and applications

EXAMPLE C, C++, Assembler.

Note 1 to entry: A typical example of systems using FVL: embedded systems.

Note 2 to entry: In the field of machinery, FVL is found in embedded software and rarely in application software.

[SOURCE: IEC 61511-1:2003, 3.2.80.1.3, modified.]

3.1.36
application software
software specific to the application, implemented by the machine manufacturer, and generally containing logic sequences, limits and expressions that control the appropriate inputs, outputs, calculations and decisions necessary to meet the SRP/CS requirements

3.1.37
embedded software
firmware
system software
software that is part of the system supplied by the control manufacturer and which is not accessible for modification by the user of the machinery

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

3.1.38
high demand or continuous mode
mode of operation in which the frequency of demands on a SRP/CS is greater than one per year or the safety related control function retains the machine in a safe state as part of normal operation

[SOURCE: IEC 62061:2012, 3.2.27, modified.]

3.1.39
proven in use
demonstration, based on an analysis of operational experience for a specific configuration of an element, that the likelihood of dangerous systematic faults is low enough so that every safety function that uses the element achieves its required performance level (PL_r)

[SOURCE: IEC 61508-4:2010, 3.8.18, modified.]

3.2 Symbols and abbreviated terms

See Table 1.

Table 1 — Symbols and abbreviated terms

Symbol or abbreviation	Description	Definition or occurrence
a, b, c, d, e	Denotation of performance levels	Table 3
AOPD	Active optoelectronic protective device (e.g. light barrier)	Annex H
B, 1, 2, 3, 4	Denotation of categories	Table 7
B_{10D}	Number of cycles until 10 % of the components fail dangerously (for pneumatic and electromechanical components)	Annex C
Cat.	Category	3.1.2
CC	Current converter	Annex I
CCF	Common cause failure	3.1.6
DC	Diagnostic coverage	3.1.26
DC_{avg}	Average diagnostic coverage	E.2
F, F1, F2	Frequency and/or time of exposure to the hazard	A.2.2
FB	Function block	4.6.3
FVL	Full variability language	3.1.35
FMEA	Failure modes and effects analysis	7.2
I, I1, I2	Input device, e.g. sensor	6.2
i, j	Index for counting	Annex D
I/O	Inputs/outputs	Table E.1
i_{ab}, i_{bc}	Interconnecting means	Figure 4
K1A, K1B	Contactors	Annex I
L, L1, L2	Logic	6.2
LVL	Limited variability language	3.1.34
M	Motor	Annex I
MTTF	Mean time to failure	Annex C
$MTTF_D$	Mean time to dangerous failure	3.1.25
n, N, $\tilde{N}$	Number of items	6.3, D.1
N_{low}	Number of SRP/CS with PL_{low} in a combination of SRP/CS	6.3
n_{op}	Mean number of annual operations	Annex C
O, O1, O_2, OTE	Output device, e.g. actuator	6.2
P, P1, P2	Possibility of avoiding the hazard	A.2.3
PES	Programmable electronic system	3.1.22
PFH_D	average probability of dangerous failure per hour	Table 3 and Table K.1
PL	Performance level	3.1.23
PLC	Programmable logic controller	Annex I
PL_{low}	Lowest performance level of a SRP/CS in a combination of SRP/CS	6.3
PL_r	Required performance level	3.1.24
r_D	Demand rate	3.1.30
r_t	Test rate	3.1.29
RS	Rotation sensor	Annex I
S, S1, S2	Severity of injury	A.2.1
SW1A, SW1B, SW2	Position switches	Annex I

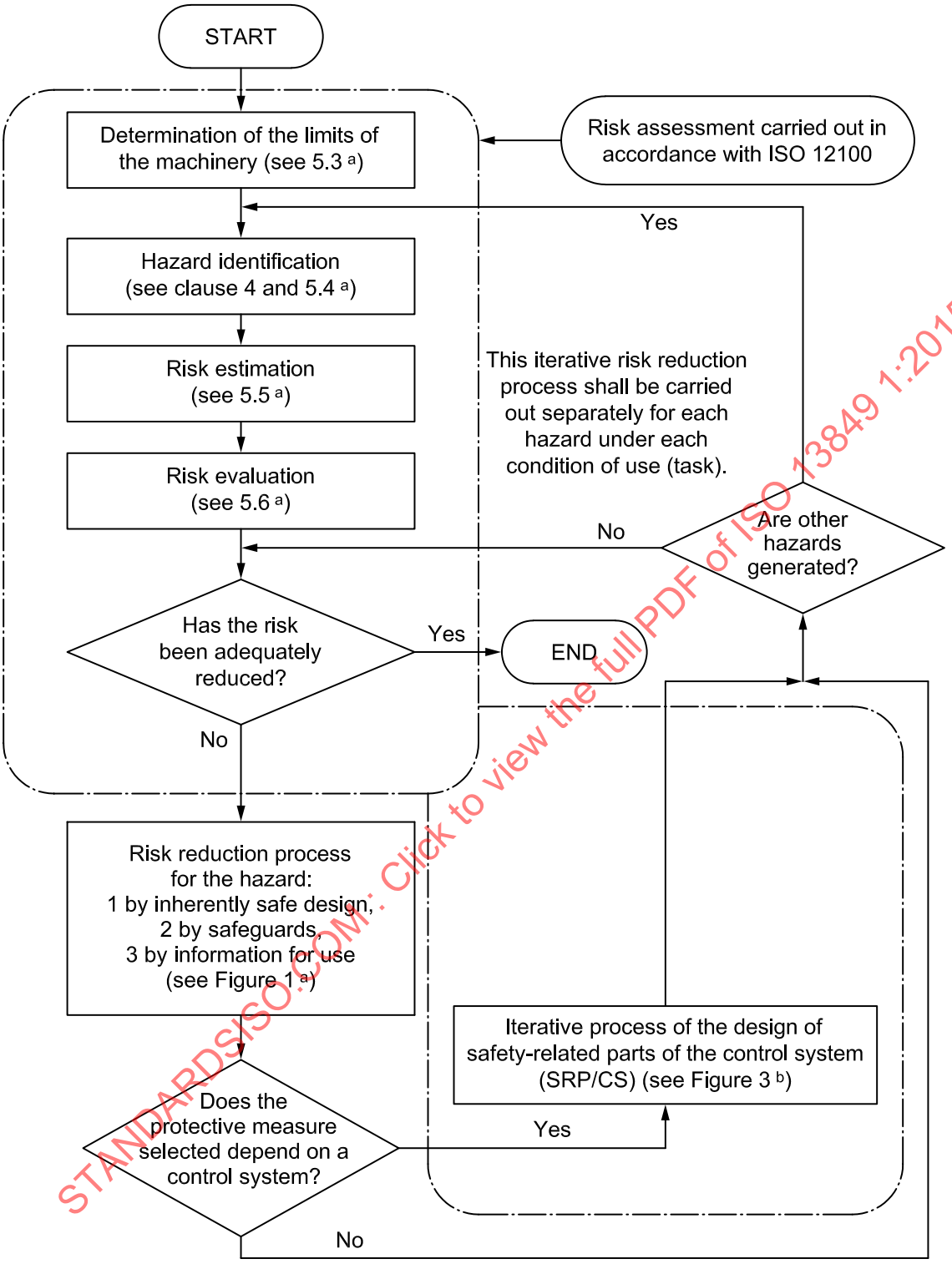
Table 1 *(continued)*

Symbol or abbreviation	Description	Definition or occurrence
SIL	Safety integrity level	Table 4
SRASW	Safety-related application software	4.6.3
SRESW	Safety-related embedded software	4.6.2
SRP	Safety-related part	General
SRP/CS	Safety-related part of a control system	3.1.1
TE	Test equipment	6.2
T_M	Mission time	3.1.28
T_{10D}	Mean time until 10 % of the components fail dangerously	Annex C

4 Design considerations

4.1 Safety objectives in design

The SRP/CS shall be designed and constructed so that the principles of ISO 12100 are fully taken into account (see Figures 1 and 3). All intended use and reasonable foreseeable misuse shall be considered.



a Refers to ISO 12100:2010

b Refers to this part of ISO 13849

Figure 1 — Overview of risk assessment/risk reduction

4.2 Strategy for risk reduction

4.2.1 General

The strategy for risk reduction at the machine is given in ISO 12100:2010, 6.1, and further guidance is given in ISO 12100:2010, 6.2 (inherent design measures) and 6.3 (safeguarding and complementary protective measures). This strategy covers the whole life cycle of the machine.

The hazard analysis and risk reduction process for a machine requires that hazards are eliminated or reduced through a hierarchy of measures:

— hazard elimination or risk reduction by design (see ISO 12100:2010, 6.2);

— risk reduction by safeguarding and possibly complementary protective measures (see ISO 12100:2010, 6.3);

— risk reduction by the provision of information for use about the residual risk (see ISO 12100:2010, 6.4).

4.2.2 Contribution to the risk reduction by the control system

The purpose in following the overall design procedure for the machine is to achieve the safety objectives (see 4.1). The design of the SRP/CS to provide the required risk reduction is an integral subset of the overall design procedure for the machine. The SRP/CS provides safety function(s) at a PL which achieves the required risk reduction. In providing safety function(s), either as an inherently safe part of the design or as a control for an interlocking guard or protective device, the design of the SRP/CS is a part of the strategy for risk reduction. This is an iterative process and is illustrated in Figures 1 and 3.

NOTE There is no need to apply this strategy of risk reduction on non-safety related parts of control systems or purely functional elements of a machine (see ISO/TR 22100-2:2013, Clause 3).

For each safety function, the characteristics (see Clause 5) and the required performance level shall be specified and documented in the safety requirements specification.

In this part of ISO 13849 the performance levels are defined in terms of probability of dangerous failure per hour. Five performance levels are set out, from the lowest PL a to the highest PL e with defined ranges of probability of a dangerous failure per hour (see Table 2).

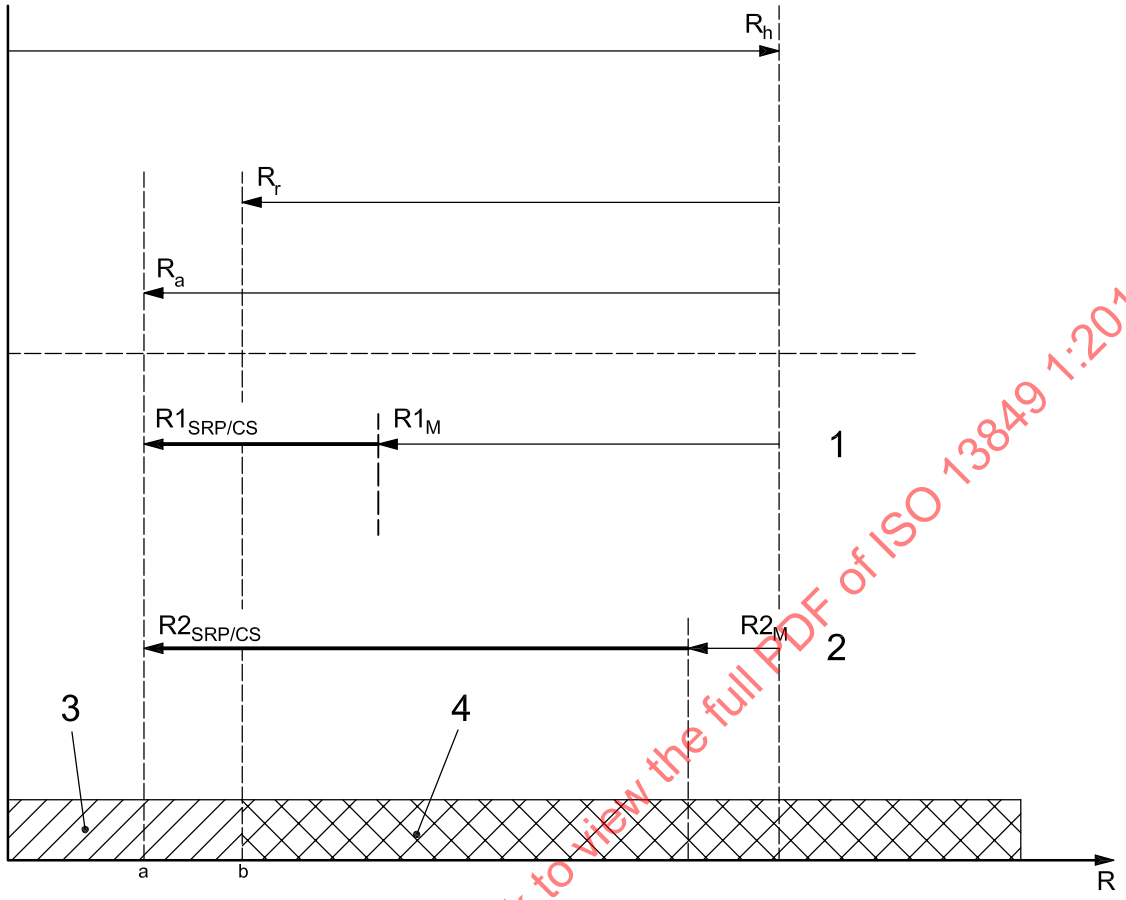
In order to achieve a PL, beside quantifiable aspects, it is also necessary to satisfy requirements related to qualitative aspects of PL (see 4.5).

Table 2 — Performance levels (PL)

PL	Average probability of dangerous failure per hour (PFH_D) 1/h
a	$\geq 10^{-5}$ to $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ to $< 10^{-6}$
e	$\geq 10^{-8}$ to $< 10^{-7}$

From the risk assessment (see ISO 12100) at the machine, the designer shall decide the contribution to the reduction of risk which needs to be provided by each relevant safety function which is carried out by the SRP/CS(s). This contribution does not cover the overall risk of the machinery under control, e.g. not the overall risk of a mechanical press, or washing machine is considered, but that part of risk reduced by the application of particular safety functions. Examples of such functions are the stopping function initiated by using an electro-sensitive protective device on a press or the door-locking function of a washing machine.

Risk reduction can be achieved by applying various protective measures (both SRP/CS and non SRP/CS) with the end result of achieving a safe condition (see Figure 2).

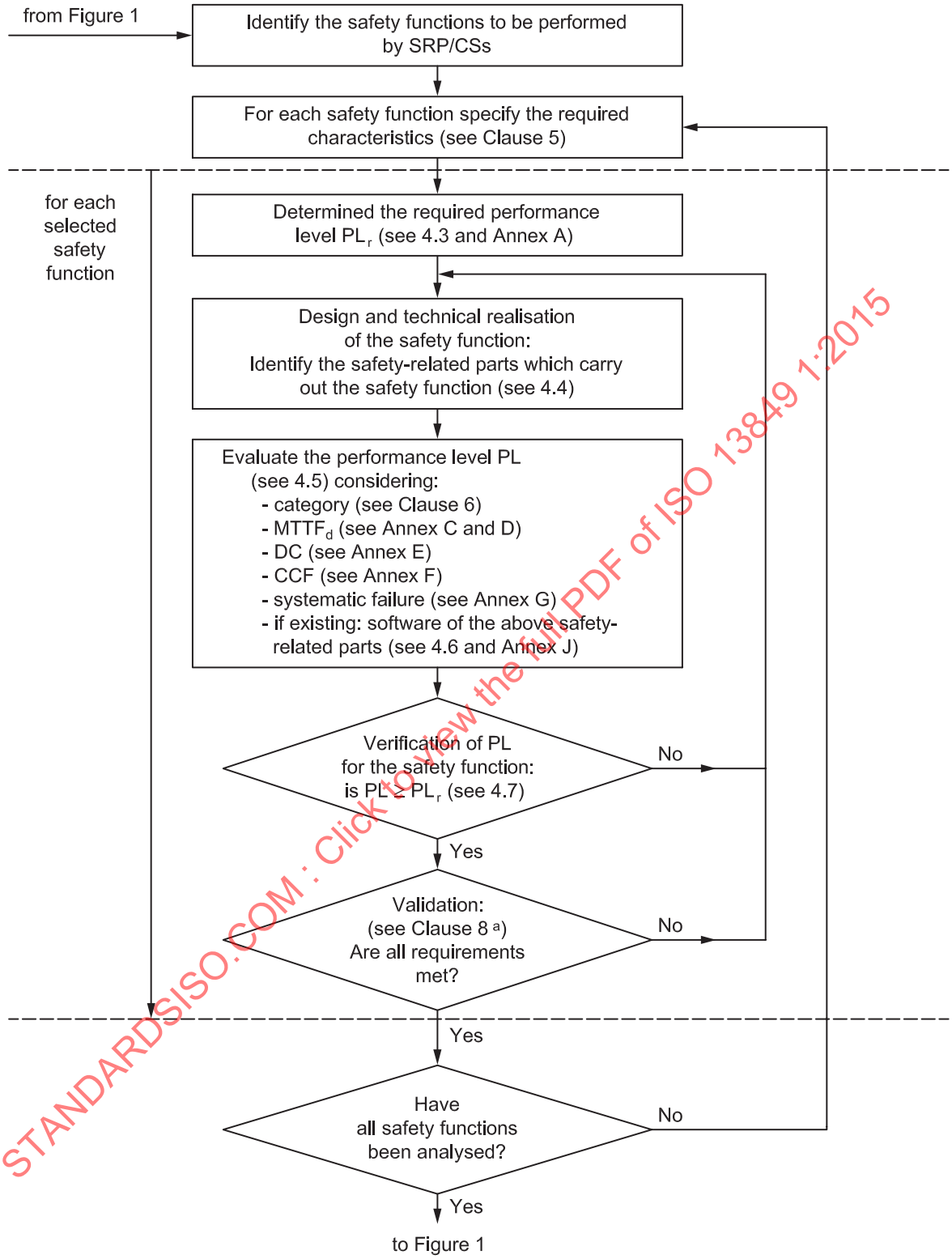


Key

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

NOTE See ISO 12100 for further information on risk reduction.

Figure 2 — Overview of the risk reduction process for each hazardous situation



a ISO 13849-2 provides additional help for the validation.

Figure 3 — Iterative process for design of safety-related parts of control systems (SRP/CS)

4.3 Determination of required performance level (PL_r)

For each selected safety function to be carried out by a SRP/CS, a required performance level (PL_r) shall be determined and documented (see Annex A for guidance on determining PL_r). The determination of

the required performance level is the result of the risk assessment and refers to the amount of the risk reduction to be carried out by the safety-related parts of the control system (see Figure 2).

The greater the amount of risk reduction required to be provided by the SRP/CS, the higher the PL_r shall be.

4.4 Design of SRP/CS

Part of the risk reduction process is to determine the safety functions of the machine. This will include the safety functions of the control system, e.g. prevention of unexpected start-up.

A safety function may be implemented by one or more SRP/CS, and several safety functions may share one or more SRP/CS [e.g. a logic unit, power control element(s)]. It is also possible that one SRP/CS implements safety functions *and* standard control functions. The designer may use any of the technologies available, singly or in combination. SRP/CS may also provide an operational function (e.g. an AOPD as a means of cycle initiation).

A typical safety function diagrammatic presentation is given in Figure 4 showing a combination of safety-related parts of control systems (SRP/CS) for

— input (SRP/CS_a),

— logic/processing (SRP/CS_b),

— output/power control elements (SRP/CS_c), and

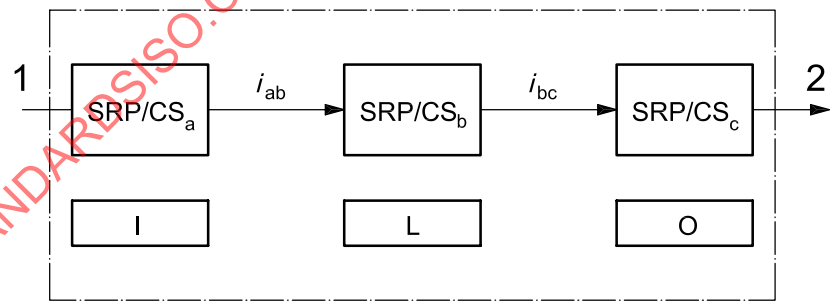
— interconnecting means (i_{ab}, i_{bc}) (e.g. electrical, optical).

NOTE 1 Within the same machinery it is important to distinguish between different safety functions and their related SRP/CS carrying out a certain safety function.

Having identified the safety functions of the control system, the designer shall identify the SRP/CS (see Figures 1 and 3) and, where necessary, shall assign them to input, logic and output and, in the case of redundancy, the individual channels, and then evaluate the performance level PL (see Figure 3).

NOTE 2 Designated architectures are given in Clause 6.

NOTE 3 All interconnecting means are included in the safety-related parts.



Key

I input (e.g. limit switch, sensor, AOPD)

L logic

O output (e.g. valve, contactor, current converter)

1 initiation event (e.g. manual actuation of a push button, opening of guard, interruption of beam of AOPD)

2 machine actuator (e.g. motor, cylinder)

Figure 4 — Diagrammatic presentation of combination of safety-related parts of control systems for processing typical safety function

4.5 Evaluation of the achieved performance level PL and relationship with SIL

4.5.1 Performance level PL

For the purposes of this part of ISO 13849, the ability of safety-related parts to perform a safety function is expressed through the determination of the performance level.

For each selected SRP/CS and/or for the combination of SRP/CS that performs a safety function the estimation of PL shall be done.

The PL of the SRP/CS shall be determined by the estimation of the following aspects:

— the $MTTF_D$ value for single components (see Annex C and Annex D);

— the DC (see Annex E);

— the CCF (see Annex F);

— the structure (see Clause 6);

— the behaviour of the safety function under fault condition(s) (see Clause 6);

— safety-related software (see 4.6 and Annex J);

— systematic failure (see Annex G);

— the ability to perform a safety function under expected environmental conditions.

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

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

a) quantifiable aspects ($MTTF_D$ value for single components, DC, CCF, structure);

b) non-quantifiable, qualitative aspects which affect the behaviour of the SRP/CS (behaviour of the safety function under fault conditions, safety-related software, systematic failure and environmental conditions).

Among the quantifiable aspects, the contribution of reliability (e.g. $MTTF_D$, structure) can vary with the technology used. For example, it is possible (within certain limits) for a single channel of safety-related parts of high reliability in one technology to provide the same or higher PL as a fault-tolerant structure of lower reliability in another technology.

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

To make the assessment of the quantifiable aspects of the PL easier, this part of ISO 13849 provides a simplified method based on the definition of five designated architectures that fulfil specific design criteria and behaviour under a fault condition (see 4.5.4).

For a SRP/CS or combination of SRP/CS designed according to the requirements given in Clause 6, the average probability of a dangerous failure could be estimated by means of Figure 5 and the procedure given in Annexes A to H, J and K.

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

In applications where the SRP/CS can be considered simple, and the required performance level is a to c, a qualitative estimation of the PL may be justified in the design rationale (see also 4.5.5).

NOTE 2 For the design of complex control systems, such as PES designed to perform safety functions, the application of other relevant standards can be appropriate (e.g. IEC 61508 or IEC 61496).

The achievement of qualitative aspects of the PL can be demonstrated by the application of the recommended measures given in 4.6 and Annex G.

In standards in accordance with IEC 61508, the ability of safety-related control systems to perform a safety function is given through a SIL. Table 3 displays the relationship between the two concepts (PLs and SILs).

PL a has no correspondence on the SIL scale and is mainly used to reduce the risk of slight, normally reversible, injury. Since SIL 4 is dedicated to catastrophic events possible in the process industry, this range is not relevant for risks at machines. Thus PL e corresponding to SIL 3 is defined as the highest level.

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

PL	SIL (IEC 61508–1, for information) high/continuous mode of operation
a	No correspondence
b	1
c	1
d	2
e	3

When a safety-related control function is designed using one or more SRP/CS, each SRP/CS shall be designed either according to this part of ISO 13849 or according to IEC 62061/IEC 61508 (see also ISO/TR 23849) — although there is correspondence between the PLs of this part of ISO 13849 and the SILs of IEC 61508 and IEC 62061. SRP/CSs are to be combined according to 6.3.

Therefore, protective measures to reduce the risk shall be applied, principally the following.

— Reduce the probability of faults at the component level. The aim is to reduce the probability of faults or failures which affect the safety function. This can be done by increasing the reliability of components, e.g. by selection of well-tried components and/or applying well-tried safety principles, in order to minimize or exclude critical faults or failures (see ISO 13849-2).

— Improve the structure of the SRP/CS. The aim is to avoid the dangerous effect of a fault. Some faults may be detected and a redundant and/or monitored structure could be needed.

Both measures can be applied separately or in combination. With some technologies, risk reduction can be achieved by selecting reliable components and by fault exclusions; but with other technologies, risk reduction could require a redundant and/or monitored system. In addition, common cause failures (CCF) shall be taken into account (see Figure 3).

For architectural constraints, see Clause 6.

4.5.2 Mean time to dangerous failure of each channel ($MTTF_D$)

The value of the $MTTF_D$ of each channel is given in three levels (see Table 4) and shall be taken into account for each channel (e.g. single channel, each channel of a redundant system) individually.

For each SRP/CS (subsystem) according to Table 5, the maximum value of $MTTF_D$ for each channel is 100 years. For Category 4 SRP/CS (subsystems) the maximum value of $MTTF_D$ for each channel is increased to 2 500 years.

NOTE 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 (SRP/CS) with Category 4 and achieve PL e in accordance with 6.3.

Table 4 — Mean time to dangerous failure of each channel ($MTTF_D$)

$MTTF_D$	
Denotation of each channel	**Range of each channel**
Low	3 years ≤ $MTTF_D$ < 10 years
Medium	10 years ≤ $MTTF_D$ < 30 years
High	30 years ≤ $MTTF_D$ ≤ 100 years
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 SRP/CS 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 SRP/CS for high risks should not depend on the reliability of components alone. To reinforce the SRP/CS against systematic and random failure, additional means such as redundancy and testing should be required. To be practicable, the number of ranges was restricted to three. The limitation of $MTTF_D$ of each channel values to a maximum of 100 years refers to the single channel of the SRP/CS which carries out the safety function. Higher $MTTF_D$ values can be used for single components (see Table D.1).	
NOTE 2 The indicated borders of this table are assumed within an accuracy of 5 %.	

For the estimation of $MTTF_D$ of a component, the hierarchical procedure for finding data shall be, in the order given:

a) use manufacturer's data;

b) use methods in Annex C and Annex D;

c) choose 10 years.

4.5.3 Diagnostic coverage (DC)

The value of the DC is given in four levels (see Table 5).

For the estimation of DC, in most cases, failure mode and effects analysis (FMEA, see IEC 60812) or similar methods can be used. In this case, all relevant faults and/or failure modes should be considered. For a simplified approach to estimating DC, see Annex E.

NOTE Examples of estimation of the diagnostic coverage (DC) are given in Annex E.

Table 5 — Diagnostic coverage (DC)

DC	
Denotation	**Range**
None	DC < 60 %
Low	60 % ≤ DC < 90 %
Medium	90 % ≤ DC < 99 %
High	99 % ≤ DC
NOTE 1 For SRP/CS consisting of several parts an average value DC_{avg} for DC is used in Figure 5, Clause 6 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 (e.g. IEC 61508) dealing with diagnostic coverage 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 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 borders of this table are assumed within an accuracy of 5 %.	

4.5.4 Simplified procedure for estimating the quantifiable aspects of PL

The PL may be estimated by taking into account all relevant parameters and the appropriate methods for calculation (see 4.5.1).

This clause describes a simplified procedure for estimating the quantifiable aspects of PL of a SRP/CS based on designated architectures. Some other architectures with similar structure may be transformed to these designated architectures in order to obtain an estimation of the PL.

The designated architectures are represented as block diagrams, and are listed in the context of each category in 6.2. Information about the block method and the safety-related block diagrams are given in 6.2 and Annex B.

The designated architectures show a logical representation of the system structure for each category. The technical realization or, for example, the functional circuit diagram, may look completely different.

The designated architectures are drawn for the combined SRP/CS, starting at the points where the safety-related signals are initiated and ending at the output of the power control elements (see also ISO 12100:2010, Annex A). The designated architectures can also be used to describe a part or subpart of a control system that responds to input signals and generates safety-related output signals. Thus the "input" element can represent, for example, a light curtain (AOPD) as well as input circuits of control logic elements or input switches. "Output" can also represent, for example, an output signal switching device (OSSD) or outputs of laser-scanners.

For the designated architectures, the following typical assumptions are made:

— mission time, 20 years (see Clause 10);

— constant failure rates within the mission time;

— for category 2, demand rate ≤ 1/100 test rate (see also Note in Annex K); 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);

— for category 2, $MTTF_D$ of the testing channel is greater than one half of $MTTF_D$ of the functional channel.

The methodology considers the categories as architectures with defined DC_{avg}. The PL of each SRP/CS depends on the architecture, the mean time to dangerous failure ($MTTF_D$) in each channel and the DC_{avg}.

Common cause failures (CCF) should also be taken into account (for guidance, see Annex F).

For SRP/CS with software, the requirements of 4.6 shall be applied .

If quantitative data are not available or not used (e.g. low complexity systems), the worst case of all relevant parameters should be chosen.

A combination of SRP/CS or a single SRP/CS may have a PL. The combination of several SRP/CS with different PL is considered in 6.3.

In the case of applications with PL_r a to c, measures to avoid faults can be sufficient; for higher risk applications, PL_r d to e, the structure of the SRP/CS can provide measures for avoiding, detecting or tolerating faults. Practical measures include redundancy, diversity, monitoring (see also ISO 12100:2010, Clause 3 and IEC 60204-1:2005).

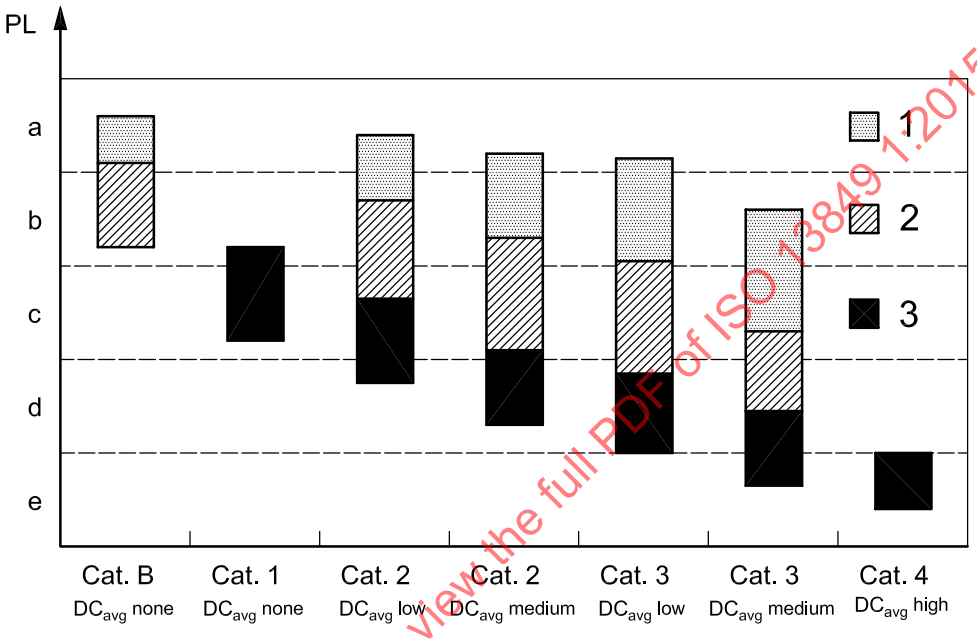
Figure 5 shows the procedure for the selection of categories in combination with the $MTTF_D$ of each channel and DC_{avg} to achieve the required PL of the safety function.

For the estimation of the PL, Figure 5 gives the different possible combinations of category with DC_{avg} (horizontal axis) and the $MTTF_D$ of each channel (bars). The bars 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 5 (which represents results of different Markov models based on designated architectures of Clause 6), the category of the SRP/CS as well as DC_{avg} and the $MTTF_D$ of each channel shall be determined (see Clause 6 and Annexes C to E).

For categories 2, 3 and 4, sufficient measures against common cause failure shall be carried out (for guidance, see Annex F). Taking these parameters into account, Figure 5 provides a graphical method for determining the PL, achieved by the SRP/CS. The combination of category (including common cause failure) and DC_{avg} determines which column of Figure 5 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 position of this area determines the achieved PL which can be read off the vertical axis. If the area covers two or three possible PLs, the PL achieved is given in Table 6. For a more precise numerical selection of PL depending on the precise value of $MTTF_D$ of each channel, see Annex K.



Key

PL performance level

1 $MTTF_D$ of each channel = low

2 $MTTF_D$ of each channel = medium

3 $MTTF_D$ of each channel = high

Figure 5 — Relationship between categories, DC_{avg}, $MTTF_D$ of each channel and PL

Table 6 — Simplified procedure for evaluating PL achieved by SRP/CS

Category	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC_{avg}	**none**	**none**	**low**	**medium**	**low**	**medium**	**high**
$MTTF_D$ of each channel							
Low	a	Not covered	a	b	b	c	Not covered
Medium	b	Not covered	b	c	c	d	Not covered
High	Not covered	c	c	d	d	d	e

4.5.5 Description of the output part of the SRP/CS by category

If for mechanical, hydraulic or pneumatic components (or components comprising a mixture of technologies) no application–specific reliability data are available, the machine manufacturer may evaluate the quantifiable aspects of the PL without any $MTTF_D$-calculation.

For such cases, the safety-related performance level (PL) is implemented by the architecture, the diagnostic and the measures against CCF.

Table 7 shows the relationship between achievable PL (corresponding to Figure 5) and categories. PL a and PL b can be implemented with Cat. B. PL c can be implemented with Cat. 1 or Cat. 2, if well-tried components and well-tried safety principles are used.

When implementing an PL c safety function with Cat.1, the T10d values of safety-relevant components that are not monitored in the process, are determined. This T10d values can be determined based on proven in use data by machine manufacturer.

The $MTTF_D$ of the test channel in Cat. 2 shall at least be 10 years.

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

Basically: In the implementation of the safety function with Cat. 2, Cat. 3 or Cat. 4 common-cause failures (CCF) and a sufficient diagnostic coverage (DC) have to be considered (low, medium for Cat. 2 and 3, high for Cat. 4).

In this case the calculation of the DC_{avg} is reduced to the arithmetic mean value of all components individuals DCs in the functional channel.

Table 7 — PL and PFH_D as worst case estimation based on category, DC_{avg}, and use of well-tried components

	PFH_D (1/h)	Cat. B	Cat. 1	Cat. 2	Cat. 3	Cat. 4
PL a	2*10–5	•	0	0	0	0
PL b	5*10–6	•	0	0	0	0
PL c	1,7*10–6	-	**•2***	**•1***	0	0
PL d	2,9*10–7	-	-	-	**•1***	0
PL e	4,7*10–8	-	-	-	-	**•1***

• Applied category is recommended.

0 Applied category is optional.

- Category is not allowed.

1* Proven in use (see 3.1.39) or well-tried (confirmed by the component manufacturer to be suitable for the particular application) components and well-tried safety principles must be used.

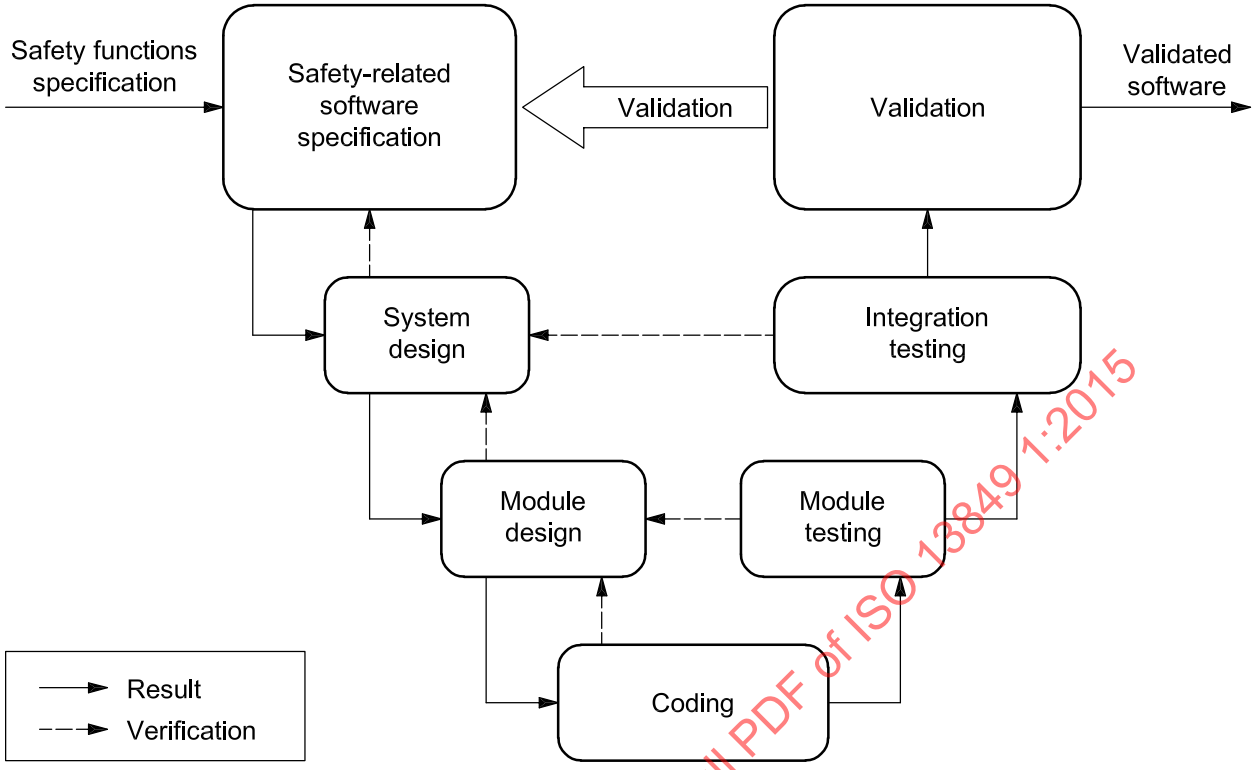
2* Well-tried components and well-tried safety principles must be used.

For safety-related components that are not monitored in the process, the T10d value can be determined based on proven in use data by the machine manufacturer.

4.6 Software safety requirements

4.6.1 General

All lifecycle activities of safety-related embedded or application software shall primarily consider the avoidance of faults introduced during the software lifecycle (see Figure 6). The main objective of the following requirements is to have readable, understandable, testable and maintainable software.



NOTE Annex J gives more detailed recommendations for lifecycle activities.

Figure 6 — Simplified V-model of software safety lifecycle

4.6.2 Safety-related embedded software (SRESW)

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

— software safety lifecycle with verification and validation activities, see Figure 6;

— documentation of specification and design;

— modular and structured design and coding;

— control of systematic failures (see G.2);

— where using software-based measures for control of random hardware failures, verification of correct implementation;

— functional testing, e.g. black box testing;

— appropriate software safety lifecycle activities after modifications.

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

— project management and quality management system comparable to, e.g. IEC 61508 or ISO 9001;

— documentation of all relevant activities during software safety lifecycle;

— configuration management to identify all configuration items and documents related to a SRESW release;

— structured specification with safety requirements and design;

— use of suitable programming languages and computer-based tools with confidence from use;

— modular and structured programming, separation from non-safety-related software, limited module sizes with fully defined interfaces, use of design and coding standards;

— coding verification by walk-through/review with control flow analysis;

— extended functional testing, e.g. grey box testing, performance testing or simulation;

— impact analysis and appropriate software safety lifecycle activities after modifications.

SRESW for components with PL_r = e shall comply with IEC 61508-3:1998, Clause 7, appropriate for SIL 3. When using diversity in specification, design and coding, for the two channels used in SRP/CS with category 3 or 4, PL_r = e can be achieved with the above-mentioned measures for PL_r of c or d.

NOTE 1 For a detailed description of such measures, see, e.g. IEC 61508–7:2000.

NOTE 2 For SRESW with diversity in design and coding, for components used in SRP/CS with category 3 or 4, 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.

For components for which SRESW requirements are not fulfilled, e.g. PLCs without safety rating by the manufacturer, these components may be used under the following alternative conditions:

— the SRP/CS is limited to PL a or b and uses category B, 2 or 3;

— the SRP/CS is limited to PL c or d and may use multiple components for two channels in category 2 or 3. The components of these two channels use diverse technologies.

4.6.3 Safety-related application software (SRASW)

The software safety lifecycle (see Figure 6) applies also to SRASW (see Annex J).

SRASW written in LVL and complying with the following requirements can achieve a PL a to e. If SRASW is written in FVL, the requirements for SRESW shall apply and PL a to e is achievable. 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, see Figure 6;

— 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) are required or recommended.

a) The safety-related software specification shall be reviewed (see also Annex J), made available to every person 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) hardware architecture with external signal interfaces, and

4) detection and control of external failure.

b) Selection of tools, libraries, languages:

1) Suitable tools with confidence from use: for PL = e achieved with one component and its tool, the tool shall comply with the appropriate safety standard; if two diverse components with diverse tools are used, confidence from use may be sufficient. Technical features which detect conditions that could cause systematic error (such as data type mismatch, ambiguous dynamic memory allocation, incomplete called interfaces, recursion, pointer arithmetic) shall be used. Checks should 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.

2) Whenever reasonable and practicable, validated function block (FB) libraries should be used — either safety-related FB libraries provided by the tool manufacturer (highly recommended for PL = e) or validated application specific FB libraries and in conformity with this part of ISO 13849.

3) A justified LVL-subset suitable for a modular approach should be used, e.g. accepted subset of IEC 61131-3 languages. Graphical languages (e.g. function block diagram, ladder diagram) are highly recommended.

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,

3) function blocks of limited size of coding,

4) code execution inside function block which should have one entry and one exit point,

5) architecture model of three stages, Inputs ⇒ Processing ⇒ Outputs (see Figure 7 and Annex J),

6) assignment of a safety output at only one program location, and

7) use of techniques for detection of external failure and for defensive programming within input, processing and output blocks which lead to safe state.

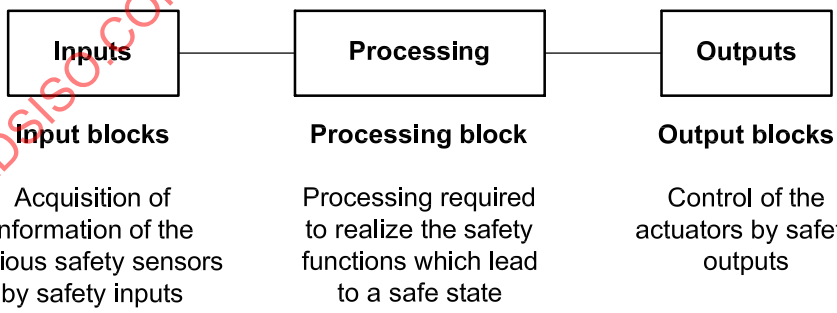


Figure 7 — General architecture model of software

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 data links;

2) there shall be no logical combination of non-safety-related and safety-related data which could 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 by control 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 is recommended and 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 and version of used library function blocks, and sufficient comments of networks/statement and declaration lines.

h) Verification[1)]

EXAMPLE Review, inspection, walkthrough or other appropriate activities.

i) Configuration management

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

After modifications of SRASW, impact analysis shall be performed to ensure specification. Appropriate lifecycle activities shall be performed after modifications. Access rights to modifications shall be controlled and modification history shall be documented.

NOTE Modification does not affect systems already in use.

4.6.4 Software-based parameterization

Software-based parameterization of safety-related parameters shall be considered as a safety-related aspect of SRP/CS design to be described in the software safety requirements specification. Parameterization shall be carried out using a dedicated software tool provided by the supplier of the

1) Verification is only necessary for application-specific code, and not for validated library functions.

SRP/CS. This tool shall have its own identification (name, version, etc.) and shall prevent unauthorized modification, for example, by use of a password.

The integrity of all data used for parameterization shall be maintained. This shall be achieved by applying measures to

— control the range of valid inputs,

— control data corruption before transmission,

— control the effects of errors from the parameter transmission process,

— control the effects of incomplete parameter transmission, and

— control the effects of faults and failures of hardware and software of the tool used for parameterization.

The parameterization tool shall fulfil all requirements for SRP/CS according to this part of ISO 13849. Alternatively, 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

— retransmission of the modified parameters to the parameterization tool, or

— other suitable means of confirming the integrity of the parameters,

as well as subsequent confirmation, e.g. by a suitably skilled person and by means of an automatic check by a parameterization tool.

NOTE 1 This is of particular importance where parameterization is carried out using a device not specifically intended for the 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.

Documentation of software-based parameterization shall indicate data used (e.g. pre-defined parameter sets) and information necessary to identify the parameters associated with the SRP/CS, the person(s) carrying out the parameterization together with other relevant information such as date of parameterization.

The following verification activities shall be applied for software based parameterization:

— 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 use of invalid values, etc.;

— verification that unauthorized modification of safety-related parameters is prevented;

— verification that the data/signals for parameterization are generated and processed in such a way that faults cannot lead to a loss of the safety function.

NOTE 2 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).

4.7 Verification that achieved PL meets PL_r

For each individual safety function the PL of the related SRP/CS shall match the required performance level (PL_r) determined according to 4.3 (see Figure 3). If this is not the case, an iteration in the process described in Figure 3 is necessary.

The PL of the different SRP/CS which are part of a safety function shall be greater than or equal to the required performance level (PL_r) of this safety function.

4.8 Ergonomic aspects of design

The interface between operators and the SRP/CS shall be designed and realized such that no person is endangered during all intended use and reasonable foreseeable misuse of the machine [see also ISO 12100, EN 614-1, ISO 9355-1, ISO 9355-2, ISO 9355-3, EN 1005-3, IEC 60204-1:2005, Clause 10, IEC 60447 and IEC 61310].

Ergonomic principles shall be used so that the machine and the control system, including the safety-related parts, are easy to use, and so that the operator is not tempted to act in a hazardous manner.

The safety requirements for observing ergonomic principles given in ISO 12100:2010, 6.2.8, apply.

5 Safety functions

5.1 Specification of safety functions

This clause provides a list and details of safety functions which can be provided by the SRP/CS. The designer (or type-C standard maker) shall include those necessary to achieve the measures of safety required of the control system for the specific application.

EXAMPLE Safety-related stop function, prevention of unexpected start-up, manual reset function, muting function, hold-to-run function.

NOTE Machinery control systems provide operational and/or safety functions. 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.

Tables 8 and 9 list some typical safety functions and, respectively, certain of their characteristics and safety-related parameters, while making reference to other International Standards whose requirements relate to the safety function, characteristic or parameter. The designer (or type-C standard maker) shall ensure that all applicable requirements are satisfied for the relevant safety functions listed in the tables.

Additional requirements are set out in this clause for certain of the safety function characteristics .

Where necessary, the requirements for characteristics and safety functions shall be adapted for use with different energy sources.

As most of the references in Tables 8 and 9 relate to electrical standards, the applicable requirements will need to be adapted in the case of other technologies (e.g. hydraulic, pneumatic).

Table 8 — Some International Standards applicable to typical machine safety functions and certain of their characteristics

Safety function/ characteristic	Requirement(s)		For additional information, see:
	This part of ISO 13849	ISO 12100:2010	
Safety-related stop function initiated by safeguard [a]	5.2.1	3.28.8, 6.2.11.3	IEC 60204–1:2005, 9.2.2, 9.2.5.3, 9.2.5.5 ISO 14119 ISO 13855
Manual reset function	5.2.2	—	IEC 60204–1:2005, 9.2.5.3, 9.2.5.4
Start/restart function	5.2.3	6.2.11.3, 6.2.11.4	IEC 60204–1:2005, 9.2.1, 9.2.5.1, 9.2.5.2, 9.2.6
Local control function	5.2.4	6.2.11.8, 6.2.11.10	IEC 60204–1:2005, 10.1.5
Muting function	5.2.5	—	IEC/TS 62046:2008, 5.5
Hold-to-run function		6.2.11.8 b)	IEC 60204–1:2005, 9.2.6.1
Enabling device function		—	IEC 60204–1:2005, 9.2.6.3, 10.9
Prevention of unexpected start-up	—	6.2.11.4	ISO 14118 IEC 60204–1:2005, 5.4
Escape and rescue of trapped persons	—	6.3.5.3	
Isolation and energy dissipation function	—	6.3.5.4	ISO 14118 IEC 60204–1:2005, 5.3, 6.3.1
Control modes and mode selection	—	6.2.11.8, 6.2.11.10	IEC 60204–1: 2005, 9.2.3, 9.2.4
Interaction between different safety-related parts of control systems	—	6.2.11.1 (last sentence)	IEC 60204–1:2005, 9.3.4
Monitoring of parameterization of safety-related input values	4.6.4	—	—
Emergency stop function [b]	—	6.3.5.2	ISO 13850 IEC 60204–1:2005, 9.2.5.4

[a] Including interlocked guards and limiting devices (e.g. overspeed, overtemperature, overpressure).

[b] Complementary protective measure, see ISO 12100:2010.

Table 9 — Some International Standards giving requirements for certain safety functions and safety-related parameters

Safety function/ safety-related parameter	Requirement		For additional information, see:
	This part of ISO 13849	ISO 12100:2010	
Response time	5.2.6	—	ISO 13855:2010, 3.2, A.3, A.4
Safety-related parameter such as speed, temperature or pressure	5.2.7	6.2.11.8 e)	IEC 60204–1:2005, 7.1, 9.3.2, 9.3.4
Fluctuations, loss and restoration of power sources	5.2.8	6.2.11.8 e)	IEC 60204–1:2005, 4.3, 7.1, 7.5
Indications and alarms	—	6.2.8	ISO 7731 ISO 11428 ISO 11429 IEC 61310–1 IEC 60204–1:2005, 10.3, 10.4 IEC 61131 IEC 62061

When identifying and specifying the safety function(s), the following shall at least be considered:

a) results of the risk assessment for each specific hazard or hazardous situation;

b) machine operating characteristics, including

- intended use of the machine (including reasonable foreseeable misuse),
- modes of operation (e.g. local mode, automatic mode, modes related to a zone or part of the machine),
- cycle time, and
- response time;

c) emergency operation;

d) description of the interaction of different working processes and manual activities (repairing, setting, cleaning, trouble shooting, etc.);

e) the behaviour of the machine that a safety function is intended to achieve or to prevent;

f) the behaviour of the machine on the loss of power (see also 5.2.8);

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

g) condition(s) (e.g. operating mode) of the machine in which it is to be active or disabled;

h) the frequency of operation;

i) priority of those functions that can be simultaneously active and that can cause conflicting action.

5.2 Details of safety functions

5.2.1 Safety-related stop function

The following applies in addition to the requirements of Table 8.

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 stop shall have priority over a stop for operational reasons.

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

NOTE A safety-related stop function can cause operational problems and a difficult restart, e.g. in an arc welding application. To reduce the temptation to defeat this stop function, it can be preceded with a stop for operational reasons to finalize the actual operation and prepare for an easy and quick restart from the stop position (e.g. without any damage of the production). One solution is the use of interlocking device with guard locking where the guard locking is released when the cycle has reached a defined position where the easy restart is possible.

5.2.2 Manual reset function

The following applies in addition to the requirements of Table 8.

After a stop command has been initiated by a safeguard, the stop condition shall be maintained until safe conditions for restarting exist.

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 deliberate action (manual reset).

The manual reset function shall

— be provided through a separate and manually operated device within the SRP/CS,

— only be achieved if all safety functions and safeguards are operative,

— not initiate motion or a hazardous situation by itself,

— be by deliberate action,

— enable the control system for accepting a separate start command,

— only be accepted by disengaging the actuator from its energized (on) position.

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

The reset actuator shall be situated outside the danger zone and in a safe position from which there is good visibility for checking that no person is within the danger zone.

Where the visibility of the danger zone is not complete, a special reset procedure is required.

NOTE One solution is the use of a second reset actuator. The reset function is initiated within the danger zone by the first actuator in combination with a second reset actuator located outside the danger zone (near the safeguard). This reset procedure needs to be realized within a limited time before the control system accepts a separate start command.

5.2.3 Start/restart function

The following applies in addition to the requirements of Table 8.

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

These requirements for start and restart shall also apply to machines which can be controlled remotely.

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

EXAMPLE In automatic machine operations, sensor feedback signals to the control system are often used to control the process flow. If a work piece has come out of position, the process flow is stopped. If the monitoring of the interlocked safeguard is not superior to the automatic process control, there could be a danger of restarting the machine while the operator readjusts the work piece. Therefore the remotely controlled restart ought not to be allowed until the safeguard is closed again and the maintainer has left the hazardous area. The contribution of prevention of unexpected start-up provided by the control system is dependent on the result of the risk assessment.

5.2.4 Local control function

The following applies in addition to the requirements of Table 8.

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

— the means for selecting local control shall be situated outside the danger zone;

— it shall only be possible to initiate hazardous conditions by a local control in a zone defined by the risk assessment;

— switching between local and main control shall not create a hazardous situation.

5.2.5 Muting function

The following applies in addition to the requirements of Table 8.

Muting shall not result in any person being exposed to hazardous situations. During muting, safe conditions shall be provided by other means.

At the end of muting, all safety functions of the SRP/CS shall be reinstated.

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

NOTE In some applications, an indication signal of muting is necessary.

5.2.6 Response time

The following applies in addition to the requirements of Table 9.

The response time of the SRP/CS shall be determined when the risk assessment of the SRP/CS indicates that this is necessary (see also Clause 11).

NOTE 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.

5.2.7 Safety-related parameters

The following applies in addition to the requirements of Table 9.

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

If errors in manual inputting of safety-related data in programmable electronic systems can lead to a hazardous situation, then a data checking system within the safety-related control system shall be provided, e.g. check of limits, format and/or logic input values.

5.2.8 Fluctuations, loss and restoration of power sources

The following applies in addition to the requirements of Table 9.

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

6 Categories and their relation to $MTTF_D$ of each channel, DC_{avg} and CCF

6.1 General

The SRP/CS shall be in accordance with the requirements of one or more of the five categories specified in 6.2.

Categories are the basic parameters used to achieve a specific PL. They state the required behaviour of the SRP/CS in respect of its resistance to faults based on the design considerations described in Clause 4.

Category B is the basic category. The occurrence of a fault can lead to the loss of the safety function. In category 1 improved resistance to faults is achieved predominantly by selection and application of components. In categories 2, 3 and 4, improved performance in respect of a specified safety function is achieved predominantly by improving the structure of the SRP/CS. In category 2 this is provided by periodically checking that the specified safety function is being performed. In categories 3 and 4 this is provided by ensuring that the single fault will not lead to the loss of the safety function. In category 4, and whenever reasonably practicable in category 3, such faults will be detected. In category 4 the resistance to the accumulation of faults will be specified.

Table 10 gives an overview of categories of the SRP/CS, the requirements and the system behaviour in case of faults.

When considering the causes of failures in some components it is possible to exclude certain faults (see Clause 7).

The selection of a category for a particular SRP/CS depends mainly upon

— the reduction in risk to be achieved by the safety function to which the part contributes,

— the required performance level (PL_r),

— the technologies used,

— the risk arising in the case of a fault(s) in that part,

— the possibilities of avoiding a fault(s) in that part (systematic faults),

— the probability of occurrence of a fault(s) in that part and relevant parameters,

— the mean time to dangerous failure ($MTTF_D$),

— the diagnostic coverage (DC), and

— the common cause failure (CCF) in the case of categories 2, 3 and 4.

6.2 Specifications of categories

6.2.1 General

Each SRP/CS shall comply with the requirements of the relevant category, see 6.2.3 to 6.2.7.

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

The following figures show not examples but general architectures. A deviation from these architectures is always possible, but any deviation shall be justified, by means of appropriate analytical tools (e.g. Markov modelling, fault tree analysis), such that the system meets the required performance level (PL_r).

The designated architectures cannot be considered only as circuit diagrams but also as logical diagrams. For categories 3 and 4, this means that not all parts are necessarily physically redundant but that there are redundant means of assuring that a fault cannot lead to the loss of the safety function.

The lines and arrows in Figures 8 to 12 represent logical interconnecting means and logical possible diagnostic means.

6.2.2 Designated architectures

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

It is important that the PL shown in Figure 5, depending on the category, $MTTF_D$ of each channel and DC_{avg}, is based on the designated architectures. If Figure 5 is used to estimate the PL the architecture of the SRP/CS should be demonstrated to be equivalent to the designated architecture of the claimed category. Designs fulfilling the characteristics of the respective category in general are equivalent to the respective designated architecture of the category.

6.2.3 Category B

The SRP/CS shall, as a minimum, be designed, constructed, selected, assembled and combined in accordance with the relevant standards and use basic safety principles for the specific application to withstand

— the expected operating stresses, e.g. the reliability with respect to breaking capacity and frequency,

— the influence of the processed material, e.g. detergents in a washing machine, and

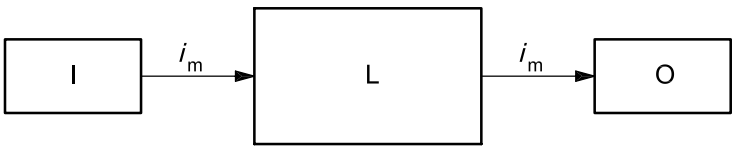
— other relevant external influences, e.g. mechanical vibration, electromagnetic interference, power supply interruptions or disturbances.

There is no diagnostic coverage (DC_{avg} = none) within category B systems and the $MTTF_D$ of each channel can be low to medium. In such structures (normally single-channel systems), the consideration of CCF is not relevant.

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

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

Specific requirements for electromagnetic compatibility are found in the relevant product standards, e.g. IEC 61800-3 for power drive systems. For functional safety of SRP/CS in particular, the immunity requirements are relevant. If no product standard exists, at least the immunity requirements of IEC 61000-6-2 should be followed.



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 B

6.2.4 Category 1

For category 1, the same requirements as those according to 6.2.3 for category B shall apply. In addition, the following applies.

SRP/CS of category 1 shall be designed and constructed using well-tried components and well-tried safety principles (see ISO 13849-2).

A "well-tried component" for a safety-related application is a component which has been either

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

b) made and verified using principles which demonstrate its suitability and reliability for safety-related applications.

Newly developed components and safety principles may be considered as equivalent to "well-tried" if they fulfil the conditions of b).

The decision to accept a particular component as being "well-tried" depends on the application.

NOTE 1 Complex electronic components (e.g. PLC, microprocessor, application-specific integrated circuit) cannot be considered as equivalent to "well tried".

The $MTTF_D$ of each channel shall be high.

The maximum PL achievable with category 1 is PL = c.

NOTE 2 There is no diagnostic coverage (DC_{avg} = none) within category 1 systems. In such structures (single-channel systems) the consideration of CCF is not relevant.

NOTE 3 When a fault occurs it can lead to the loss of the safety function. However, the $MTTF_D$ of each channel in category 1 is higher than in category B. Consequently, the loss of the safety function is less likely.

It is important that a clear distinction between "well-tried component" and "fault exclusion" (see Clause 7) be made. The qualification of a component as being well-tried depends on its application. For example, a position switch with positive opening contacts could be considered as being well-tried for a machine tool, while at the same time as being inappropriate for application in a food industry — in the milk industry, for instance, this switch would be destroyed by the milk acid after a few months. A fault exclusion can lead to a very high PL, but the appropriate measures to allow this fault exclusion should be applied during the whole lifetime of the device. In order to ensure this, additional measures outside the control system may be necessary. In the case of a position switch, some examples of these kinds of measures are

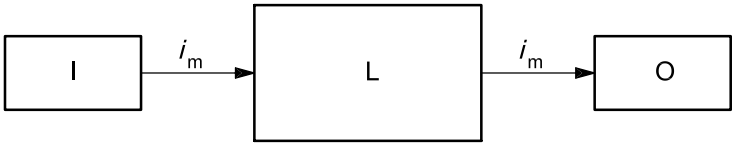
— means to secure the fixing of the switch after its adjustment,

— means to secure the fixing of the cam,

— means to ensure the transverse stability of the cam,

— means to avoid overtravel of the position switch, e.g. adequate mounting strength of the shock absorber and any alignment devices, and

— means to protect it against damage from outside.



Key

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

Figure 9 — Designated architecture for category 1

6.2.5 Category 2

For category 2, the same requirements as those according to 6.2.3 for category B shall apply. "Well–tried safety principles" according to 6.2.4 shall also be followed. In addition, the following applies.

SRP/CS of category 2 shall be designed so that their function(s) are checked at suitable intervals by the machine control system. The check of the safety function(s) shall be performed

— at the machine start-up, and

— prior to the initiation of any hazardous situation, e.g. start of a new cycle, start of other movements, immediately upon on demand of the safety function and/or periodically during operation if the risk assessment and the kind of operation shows that it is necessary.

The initiation of this check may be automatic. Any check of the safety function(s) shall either

— allow operation if no faults have been detected, or

— generate an output (OTE) which initiates appropriate control action, if a fault is detected.

For PLr = d the output (OTE) shall initiate a safe state which is maintained until the fault is cleared.

For PLr up to and including PLr = c, whenever practicable the output (OTE) shall initiate a safe state which 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 output of the test equipment OTE to provide a warning.

For the designated architecture of category 2, as shown in Figure 10, the calculation of $MTTF_D$ and DC_{avg} should take into account only the blocks of the functional channel (i.e. I, L and O in Figure 10) and not the blocks of the testing channel (i.e. TE and OTE in Figure 10).

The diagnostic coverage (DC_{avg}) of the functional channel shall be at least low. The $MTTF_D$ of each channel shall be low-to-high, depending on the required performance level (PL_r). Measures against CCF shall be applied (see Annex F).

The check 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.

The maximum PL achievable with category 2 is PL = d.

NOTE 1 In some cases category 2 is not applicable because the checking of the safety function cannot be applied to all components.

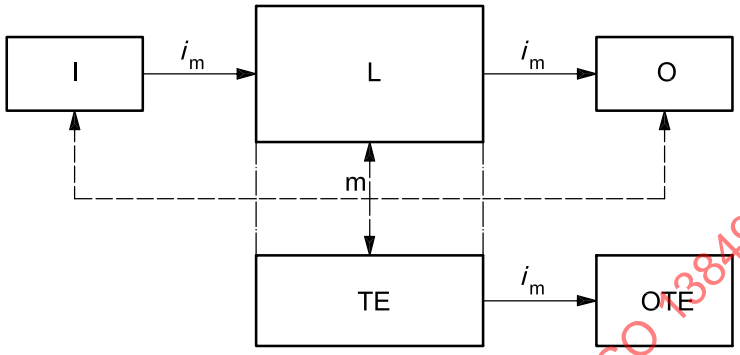
NOTE 2 Category 2 system behaviour is characterized by

— the occurrence of a fault can lead to the loss of the safety function between checks,

— the loss of safety function is detected by the check.

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 checking frequency can decrease the probability of occurrence of a dangerous situation.

NOTE 4 For applying the simplified approach based on designated architectures, refer to the assumptions in 4.5.4.



Key

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

Dashed lines represent reasonably practicable fault detection.

Figure 10 — Designated architecture for category 2

6.2.6 Category 3

For category 3, the same requirements as those according to 6.2.3 for category B shall apply. "Well-tried safety principles" according to 6.2.4 shall also be followed. In addition, the following applies.

SRP/CS of category 3 shall be designed so that a single fault in any of these parts does not lead to the loss of the safety function. Whenever reasonably practicable, the single fault shall be detected at or before the next demand upon the safety function.

The diagnostic coverage (DC_{avg}) of the total SRP/CS 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.

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

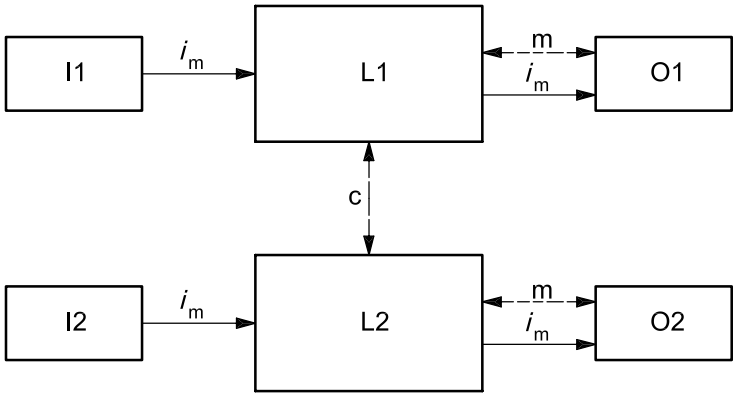
NOTE 3 Category 3 system behaviour is characterized by

— continued performance of the safety function in the presence of a single fault,

— detection of some, but not all, faults,

— possible loss of the safety function due to accumulation of undetected faults.

NOTE 4 The technology used will influence the possibilities for the implementation of fault detection.



Key

i_m	interconnecting means
c	cross monitoring
I1, I2	input device, e.g. sensor
L1, L2	logic
m	monitoring
O1, O_2	output device, e.g. main contactor

Dashed lines represent reasonably practicable fault detection.

Figure 11 — Designated architecture for category 3

6.2.7 Category 4

For category 4, the same requirements as those according to 6.2.3 for category B shall apply. "Well-tried safety principles" according to 6.2.4 shall also be followed. In addition, the following applies.

SRP/CS of category 4 shall be designed such that

— a single fault in any of these safety-related parts does not lead to a loss of the safety function, and

— the single fault is detected at or before the next demand upon the safety functions, e.g. immediately, at switch on, or at 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.

The diagnostic coverage (DC_{avg}) of the total SRP/CS shall be high, including the accumulation of faults. The $MTTF_D$ of each of the redundant channels shall be high. Measures against CCF shall be applied (see Annex F).

NOTE 1 Category 4 system behaviour is characterized by

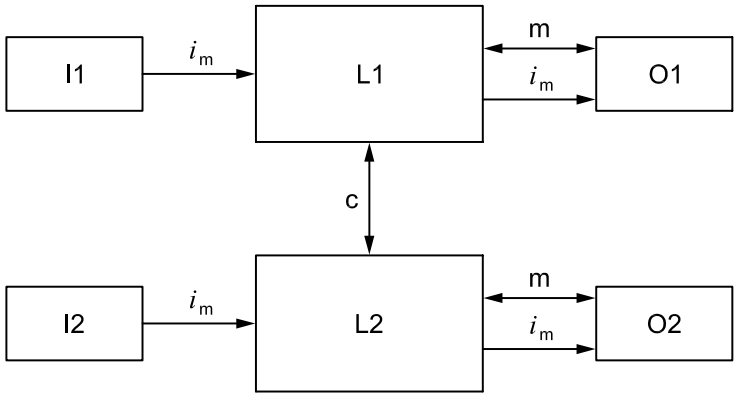
— continued performance of the safety function in the presence of a single fault,

— detection of faults in time to prevent the loss of the safety function,

— the accumulation of undetected faults is taken into account.

NOTE 2 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 may be sufficient.



Key

i_m	interconnecting means
c	cross monitoring
I1, I2	input device, e.g. sensor
L1, L2	logic
m	monitoring
O1, O_2	output device, e.g. main contactor

Solid lines for monitoring represent diagnostic coverage that is higher than in the designated architecture for category 3.

Figure 12 — Designated architecture for category 4

Table 10 — Summary of requirements for categories

Category	Summary of requirements	System behaviour	Principle used to achieve safety	$MTTF_D$ of each channel	DC_{avg}	CCF
B (see 6.2.3)	SRP/CS and/or their protective equipment, as well as their components, shall be designed, constructed, selected, assembled and combined in accordance with relevant standards so that they can withstand the expected influence. Basic safety principles shall be used.	The occurrence of a fault can lead to the loss of the safety function.	Mainly characterized by selection of components	Low to medium	None	Not relevant
1 (see 6.2.4)	Requirements of B shall apply. Well-tried components and well-tried safety principles shall be used.	The occurrence of a fault can lead to the loss of the safety function but the probability of occurrence is lower than for category B.	Mainly characterized by selection of components	High	None	Not relevant
NOTE For full requirements, see Clause 6.						

Table 10 *(continued)*

Category	Summary of requirements	System behaviour	Principle used to achieve safety	$MTTF_D$ of each channel	DC_{avg}	CCF
2 (see 6.2.5)	Requirements of B and the use of well-tried safety principles shall apply. Safety function shall be checked at suitable intervals by the machine control system (see 4.5.4).	The occurrence of a fault can lead to the loss of the safety function between the checks. The loss of safety function is detected by the check.	Mainly characterized by structure	Low to high	Low to medium	See Annex F
3 (see 6.2.6)	Requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed, so that — a single fault in any of these parts does not lead to the loss of the safety function, and — whenever reasonably practicable, the single fault is detected.	When a single fault occurs, the safety function is always performed. Some, but not all, faults will be detected. Accumulation of undetected faults can lead to the loss of the safety function.	Mainly characterized by structure	Low to high	Low to medium	See Annex F
4 (see 6.2.7)	Requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed, so that — a single fault in any of these parts does not lead to a loss of the safety function, and — the single fault is detected at or before the next demand upon the safety function, but that if this detection is not possible, an accumulation of undetected faults shall not lead to the loss of the safety function.	When a single fault occurs the safety function is always performed. Detection of accumulated faults reduces the probability of the loss of the safety function (high DC). The faults will be detected in time to prevent the loss of the safety function.	Mainly characterized by structure	High	High including accumulation of faults	See Annex F
NOTE For full requirements, see Clause 6.						

6.3 Combination of SRP/CS to achieve overall PL

A safety function can be realized by a combination of several SRP/CS: input system, signal processing unit, output system. These SRP/CS may be assigned to one and/or different categories. For each SRP/CS used, a category according to 6.2 shall be selected. For the overall combination of these SRP/CS, an overall PL may be identified using the methods described in this clause. In this case, the validation of the combination of SRP/CS is required (see Figure 3).

According to 6.2, the combined safety-related parts of a control system start at the points where the safety-related signals are initiated and end at the output of the power control elements. But the combined SRP/CS could consist of several parts connected in a linear (series alignment) or redundant (parallel alignment) way. To avoid a new complex estimation of the performance level (PL) achieved

by the combined SRP/CS where the separate PLs of all parts are already calculated, the following estimations are presented for a series combination of SRP/CS.

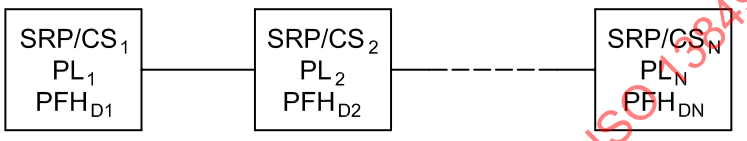
It is assumed that there are N separate SRP/CS_i in a series combination, which as a whole performs a safety function. For each SRP/CS_i, a PL_i has already been evaluated. This situation is illustrated in Figure 13 (see also Figure 4 and Figure H.2).

If the PFH_D values of all SRP/CS_i are known, then the PFH_D of the combined SRP/CS is the sum of all PFH_D values of the N individual SRP/CS_i. The PL of the combined SRP/CS is limited by:

— the lowest PL of any individual SRP/CS_i involved in performing the safety function (because the PL is determined also by non-quantifiable aspects) and

— the PL corresponding to the PFH_D of the combined SRP/CS according to Table 2.

NOTE See Annex H and ISO/TR 23849, 8.2.6 for an example of this method.



SRP/CS

PL

$$PFH_D = PFH_{D1} + PFH_{D2} + \ldots + PFH_{DN}$$

Figure 13 — Combination of SRP/CS to achieve overall PL

If the PFH_D values of all individual SRP/CS_i are not known, then as a worst case alternative to the above method, the PL of the whole combined SRP/CS performing the safety function may be calculated using Table 11 as follows:

a) Identify the lowest PL_i: this is PL_{low}.

b) Identify the number $N_{low} \leq N$ of SRP/CS_i, with $PL_i = PL_{low}$.

c) Look-up PL in Table 11.

Table 11 — Calculation of PL for series alignment of SRP/CS

PL_{low}	N_{low}	⇒	PL
a	> 3	⇒	None, not allowed
	≤ 3	⇒	a
b	> 2	⇒	a
	≤ 2	⇒	b
c	> 2	⇒	b
	≤ 2	⇒	c
d	> 3	⇒	c
	≤ 3	⇒	d
e	> 3	⇒	d
	≤ 3	⇒	e
NOTE The values calculated for this look-up table are based on reliability values at the mid-point for each PL.			

7 Fault consideration, fault exclusion

7.1 General

In accordance with the category selected, safety-related parts shall be designed to achieve the required performance level (PL_r). The ability to resist faults shall be assessed.

7.2 Fault consideration

ISO 13849-2 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 should also be clearly elaborated. For new components not mentioned in ISO 13849-2, a failure mode and effects analysis (FMEA, see IEC 60812) shall be carried out to establish the 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;

— two or more separate faults having a common cause shall be considered as a single fault (known as a CCF);

— the simultaneous occurrence of two or more faults having separate causes is considered highly unlikely and therefore need not be considered.

7.3 Fault exclusion

It is not always possible to evaluate SRP/CS without assuming that certain faults can be excluded. For detailed information on fault exclusions, see ISO 13849-2.

Fault exclusion is a compromise between technical safety requirements and the theoretical possibility of occurrence of a fault.

Fault exclusion can be based on

— the technical improbability of occurrence of some faults,

— generally accepted technical experience, independent of the considered application, and

— technical requirements related to the application and the specific hazard.

If faults are excluded, a detailed justification shall be given in the technical documentation.

8 Validation

The design of the SRP/CS shall be validated (see Figure 3). The validation shall demonstrate that the combination of SRP/CS providing each safety function meets all relevant requirements of this part of ISO 13849.

For details of validation, see ISO 13849-2.

9 Maintenance

Preventive or corrective maintenance can be necessary to maintain the specified performance of the safety-related parts. Deviations with time from the specified performance can lead to a deterioration in safety or even to a hazardous situation. The information for use of the SRP/CS shall include instructions for the maintenance (including periodic inspection) of the SRP/CS.

The provisions for the maintainability of the safety-related part(s) of a control system shall follow the principles given in ISO 12100:2010, 6.2.7. All information for maintenance shall comply with ISO 12100:2010, 6.4.5.1 e).

10 Technical documentation

When designing a SRP/CS, its designer shall document at least the following information relevant to the safety-related part:

— safety function(s) provided by the SRP/CS;

— the characteristics of each safety function;

— the exact points at which the safety-related part(s) start and end;

— environmental conditions;

— the performance level (PL);

— the category or categories selected;

— the parameters relevant to the reliability ($MTTF_D$, DC, CCF and mission time);

— measures against systematic failure;

— the technology or technologies used;

— all safety-relevant faults considered;

— justification for fault exclusions (see ISO 13849-2);

— the design rationale (e.g. faults considered, faults excluded);

— software documentation;

— measures against reasonably foreseeable misuse.

NOTE In general, this documentation is foreseen as being for the manufacturer's internal purposes and will not be distributed to the machine user.

11 Information for use

The principles of ISO 12100:2010, 6.4.5.2, and the applicable sections of other relevant documents (e.g. IEC 60204-1:2005, Clause 17), shall be applied. In particular, that information which is important for the safe use of the SRP/CS shall be given to the user. This shall include, but is not limited to the following:

— the limits of the safety-related parts to the category(ies) selected and any fault exclusions;

— the limits of the SRP/CS and any fault exclusions (see 7.3), for which, when essential for maintaining the selected category or categories and safety performance, appropriate information (e.g. for modification, maintenance and repair) shall be given to ensure the continued justification of the fault exclusion(s);

— the effects of deviations from the specified performance on the safety function(s);

— clear descriptions of the interfaces to the SRP/CS and protective devices;

— response time;

— operating limits (including environmental conditions);

— indications and alarms;

— muting and suspension of safety functions;

— control modes;

— maintenance (see Clause 9);

— maintenance check lists;

— ease of accessibility and replacing of internal parts;

— means for easy and safe trouble shooting;

— information explaining the applications for use relevant to the category to which reference is made;

— checking test intervals where relevant.

Specific information shall be provided on the category or categories and performance level of the SRP/CS, as follows:

— dated reference to this part of ISO 13849 (i.e. “ISO 13849-1:2006”);

the Category, B, 1, 2, 3, or 4;

— the performance level, a, b, c, d or e.

EXAMPLE An SRP/CS in accordance with this edition of ISO 13849-1, of Category B and performance level a, would be referred to as follows:

ISO 13849-1:2006 Category B PL a

Annex A
(informative)

Determination of required performance level (PL_r)

A.1 Selection of PL_r

Annex A is concerned with the contribution to the reduction in risk made by the safety-related parts of the control system being considered. The method given here provides only an estimation of the risk reduction required and is intended only as guidance to the designer and standard maker in determining the PL_r for each necessary safety function to be carried out by an SRP/CS.

NOTE 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 (ie, the probability of occurrence is 100 %). Other risk estimation methods for specific types of machine can be used as appropriate and experience in successfully dealing with similar machines/hazards should be taken into account when estimating PLr. Therefore, the PL required by a type-C standard can deviate from that indicated by the generic approach given at Figure A.1.

The graph at 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 PLr 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 2).

The severity of injury (denoted by S) is roughly estimated only (e.g. laceration, amputation, fatality). For the frequency of occurrence, auxiliary parameters are used to improve the estimation. These parameters are

— frequency and time of exposure to the hazard (F), and

— possibility of avoiding the hazard or limiting the harm (P).

Experience has shown that these parameters can be combined, as in Figure A.1, to give a gradation of risk from low to high. It is emphasized that this is a qualitative process giving only an estimation of risk.

A.2 Guidance for selecting parameters S, F and P for the risk estimation

A.2.1 Severity of injury S1 and S2

In estimating the risk arising from a failure of a safety function only slight injuries (normally reversible) and serious injuries (normally irreversible) and death 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.

A.2.2 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 could facilitate making the right decision where doubt exists.

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 part of ISO 13849, 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 work pieces, 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.

A.2.3 Possibility of avoiding the hazardous event P1 and P2 and probability of occurrence

The probability of avoiding the hazard and the probability of occurrence of a hazardous event are both combined in the parameter P. When a hazardous situation occurs, P1 should only be selected if there is a realistic chance of avoiding a hazard or of significantly reducing its effect; otherwise P2 should be selected.

Where the probability of occurrence of a hazardous event can be justified as low, the PL_r may be reduced by one level, see A.2.3.2.

A.2.3.1 Possibility of avoiding the hazard

It is important to know whether a hazardous situation 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:

— speed with which the hazard arises (e.g. quickly or slowly);

— possibilities for hazard avoidance (e.g. by escaping);

— practical safety experiences relating to the process;

— whether operated by trained and suitable operators;

— operated with or without supervision.

A.2.3.2 Probability of occurrence of a hazardous event

The probability of occurrence of a hazardous event depends on either human behaviour or technical failures. In most cases, the appropriate probabilities are unknown or hard to identify. The estimation of the probability of occurrence of a hazardous event should be based on factors including:

— reliability data;

— history of accidents on comparable machines.

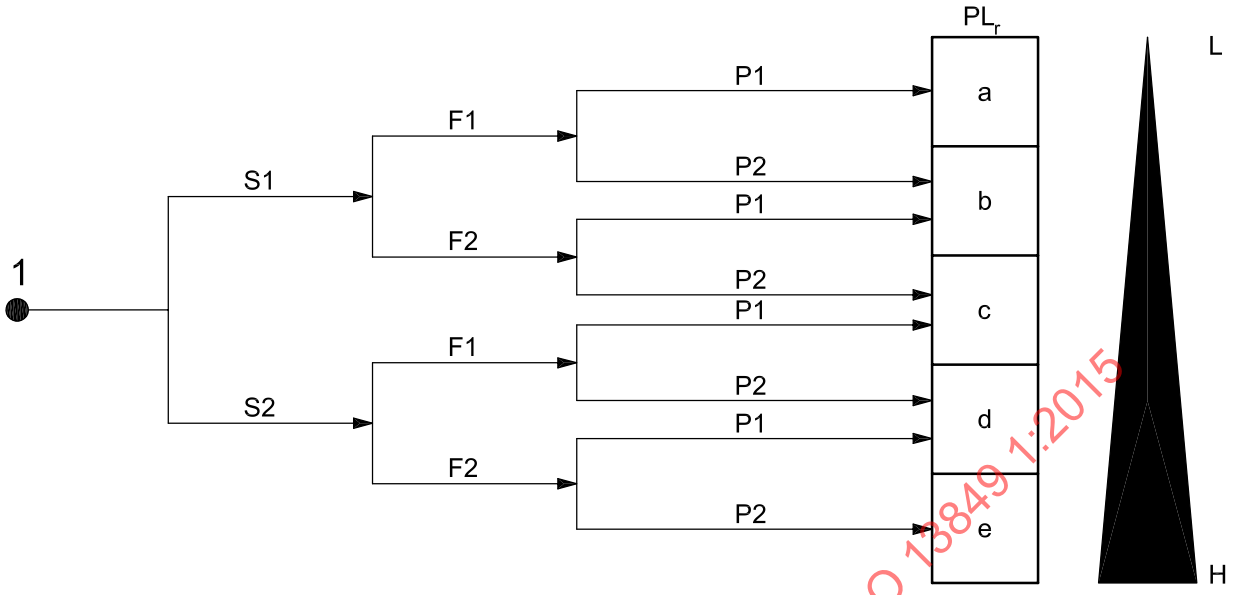
NOTE A low number of accidents does not necessarily mean that the occurrence of hazardous situations is low, but that the safety measures on the machines are sufficient.

Where comparable machines

— include the same risk(s) that the relevant safety function is intended to reduce,

— require the same process and operator action,

— apply the same technology causing the hazard.



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 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 hazard or limiting harm
P1 possible under specific conditions
P2 scarcely possible

Figure A.1 — Graph for determining required PL_r for safety function

Figure A.1 provides guidance for the determination of the safety-related PL_r depending on the risk assessment for the whole machine. The risk assessment method is based on ISO 12100 (see Figure 1 and also ISO/TR 22100-2). The graph should be considered for each safety function.

A.3 Overlapping hazards

When using ISO 13849-1, all hazards are considered as a specific hazard or hazardous situation. For the quantification of risk, 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 may create various simultaneous hazardous situations, for example 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, each robot is considered separately.

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

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 SRP/CS. The SRP/CS should be separated into a small number of blocks according to the following:

— blocks should represent logical units of the SRP/SC related to the execution of the safety function;

— different channels performing the safety function should be separated into different blocks — if one block is no longer able to perform its function, the execution of the safety function through the blocks of the other channel should not be affected;

— 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;

— each hardware unit of the SRP/CS should belong to exactly 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 failure mode and effects analysis or the parts count method, see D.1);

— hardware units only used for diagnostics (e.g. test equipment) and which do not affect the execution of the safety function in the different channels when they fail dangerously, may be separated from hardware units necessary for the execution of the safety function in the different channels.

NOTE For the purposes of this part of ISO 13849, "blocks" do not correspond to functional blocks or reliability blocks.

B.2 Safety-related block diagram

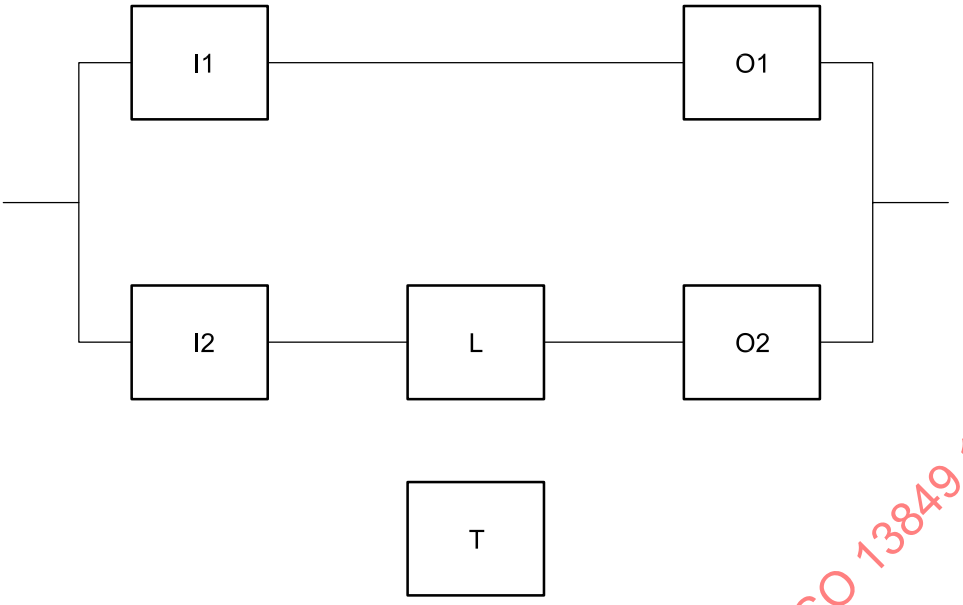
The blocks defined by the block method may be used to graphically represent the logical structure of the SRP/CS in a safety-related block diagram. For such a graphical representation, the following may be of guidance:

— 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 SRP/CS fails dangerously, the whole channel might not be able to execute the safety function any longer);

— only the dangerous failure of all channels in a parallel alignment leads to the loss of the safety function (e.g. a safety function performed by several channels is executed as long as at least one channel has no failure);

— blocks used only for testing purposes and which do not affect the execution of the safety function in the different channels 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, O_2 output devices, e.g. main contactor

T testing device

I1 and O1 build up the first channel (series alignment).

I2, L and O_2 build up the second channel (series alignment), with both channels executing the safety function redundantly (parallel alignment).

T is only used for testing.

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

Annex C
(informative)

Calculating or evaluating $MTTF_D$ values for single components

C.1 General

Annex C gives several methods for calculating or evaluating $MTTF_D$ values for single components: the method given in C.2 is based on the respect 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, or the relevant standard (see Table C.1) for the design of the component (confirmation in the data sheet 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.

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.

a) The hydraulic components are manufactured according to basic and well-tried safety principles in accordance with ISO 13849-2:2012, Tables C.1 and C.2, for the design of the hydraulic component (confirmation in the data sheet of the component).

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

b) The manufacturer of the hydraulic component specifies the appropriate application and operating conditions for the SRP/CS designer. The SRP/CS designer shall provide information pertaining to his responsibility to apply the basic and well-tried safety principles according to ISO 13849-2:2012, Tables C.1 and C.2, for the implementation and operation of the hydraulic component.

If the criteria presented in C.4 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, then the $MTTF_D$ value can be estimated higher as shown in Table C.1

But if either a) or b) is not achieved, the $MTTF_D$ value for the single hydraulic component has to 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.

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	Tables A.1 and A.2	—	$MTTF_D$ = 150
Hydraulic components with n_{op} ≥ 1 000 000 cycles per year	Tables C.1 and C.2	ISO 4413	$MTTF_D$ = 150
Hydraulic components with 1 000 000 cycles per year > n_{op} ≥ 500 000 cycles per year	Tables C.1 and C.2	ISO 4413	$MTTF_D$ = 300
Hydraulic components with 500 000 cycles per year > n_{op} ≥ 250 000 cycles per year	Tables C.1 and C.2	ISO 4413	$MTTF_D$ = 600
Hydraulic components with 250 000 cycles per year > n_{op}	Tables C.1 and C.2	ISO 4413	$MTTF_D$ = 1 200
Pneumatic components	Tables B.1 and B.2	ISO 4414	B_{10D} = 20 000 000
Relays and contactor relays with small load	Tables D.1 and D.2	EN 50205 IEC 61810 IEC 60947	B_{10D} = 20 000 000
Relays and contactor relays with nominal load	Tables D.1 and D.2	EN 50205 IEC 61810 IEC 60947	B_{10D} = 400 000
Proximity switches with small load	Tables D.1 and D.2	IEC 60947 ISO 14119	B_{10D} = 20 000 000
Proximity switches with nominal load	Tables D.1 and D.2	IEC 60947 ISO 14119	B_{10D} = 400 000
Contactors with small load	Tables D.1 and D.2	IEC 60947	B_{10D} = 20 000 000
Contactors with nominal load	Tables D.1 and D.2	IEC 60947	B_{10D} = 1 300 000 (see Note 1)
Position switches [a]	Tables D.1 and D.2	IEC 60947 ISO 14119	B_{10D} = 20 000 000
Position switches (with separate actuator, guard-locking) [a]	Tables D.1 and D.2	IEC 60947 ISO 14119	B_{10D} = 2 000 000
Emergency stop devices [a]	Tables D.1 and D.2	IEC 60947 ISO 13850	B_{10D} = 100 000

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

NOTE 1 B_{10D} is estimated as two times B_{10} (50 % dangerous failure) if no other information (e.g. product standard) is available.

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

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 SRP/CS. 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 may be possible, that the machine builder can apply a fault exclusion according to ISO 13849-2, Table D.8, considering the specific application and environmental conditions of the device.

[a] If fault exclusion for direct opening action is possible.

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)
Push buttons (e.g. enabling switches) [a]	Tables D.1 and D.2	IEC 60947	B_{10D} = 100 000
For the definition and use of B_{10D}, see C.4. NOTE 1 B_{10D} is estimated as two times B_{10} (50 % dangerous failure) if no other information (e.g. product standard) is available. NOTE 2 "Nominal load" or "small load" should take into account safety principles described in ISO 13849-2, like over-dimensioning of the rated current value. "Small load" means, for example, 20 %. 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 SRP/CS. 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 may be possible, that the machine builder can apply a fault exclusion according to ISO 13849-2, Table D.8, considering the specific application and environmental conditions of the device. [a] If fault exclusion for direct opening action is possible.			

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, etc) it may be difficult to calculate the mean time to dangerous failure ($MTTF_D$ for components), which is given in years and which is required by this part of ISO 13849. Most of the time, the manufacturers of these kinds of components only give the mean number of cycles until 10 % of the components 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 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-tried safety principles in accordance with ISO 13849-2:2012, Table A.2, Table B.2 or D.2.

   NOTE 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 shall provide information pertaining to his responsibility to fulfil the basic safety principles according to ISO 13849-2:2012, Table B.1 or D.1, for the implementation and operation of the component. For category 1, 2, 3 or 4, the user has to be informed of his responsibility to fulfil the well-tried safety principles according to ISO 13849-2:2012, Tables B.2 or 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})[2)] should be determined by the manufacturer of the component in accordance with relevant product standards for the test

2) If the dangerous fraction of B_{10} is not given (e.g. by manufacturer), 50 % of B_{10} may be used, so B_{10d} = 2 B_{10} is

methods (e.g. IEC 60957-5-1, ISO 19973, IEC 61810). The dangerous failure modes of the component have to be defined, e.g. sticking at an end position or change of switching times. If not all the components fail dangerously during the tests (e.g. seven components tested, only five fail dangerously), an analysis taking into account the components that were *not* dangerously failed components should be performed.

With B_{10D} and n_{op}, the mean number of annual operations, $MTTF_D$ for components can be calculated as

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

where

$$n_{op} = \frac{d_{op} \times h_{op} \times 3600\ s/h}{t_{cycle}} \tag{C.2}$$

with the following assumptions having been made on the application of the component:

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

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

$$T_{10D} = \frac{B_{10D}}{n_{op}} \tag{C.3}$$

NOTE Explanation of the formulas in C.4.2.

B_{10D}, the mean number of cycles till 10 % of the components fail dangerously, can be converted to T_{10D}, the mean time until 10 % of the components fail dangerously, by using n_{op}, the mean number of annual operations:

$$T_{10D} = \frac{B_{10D}}{n_{op}} \tag{C.4}$$

The reliability methods in this part of ISO 13849 assume that the failure of components is distributed exponentially over time: $F(t) = 1 - \exp(-\lambda dt)$. For pneumatic and electromechanical 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

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

Formula (C.5) 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:

$$F(T_{10D}) = 1 - \exp(-\lambda_D T_{10D}) = 10\% \quad \text{means} \quad \lambda_D = -\frac{\ln(0,9)}{T_{10D}} = \frac{0,10\,536}{T_{10D}} \approx \frac{0,1}{T_{10D}} \tag{C.6}$$

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

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

recommended.

NOTE All variables used in the equations are physical quantities expressed as the product of a numerical value and a unit of measurement. The correct application e.g. of Formulae C.5, C.6 and $MTTF_D = 1/\lambda_D$ can require the transformation of "years" to "hours" using 1 year = 8 760 h.

C.4.3 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 beginning of two successive switching of the valve is estimated as 5 s. This yields the following values:

— d_{op} of 220 days per year;

— h_{op} of 16 h per day;

— t_{cycle} of 5 s per cycle;

— B_{10D} of 60 million cycles.

With these input data the following quantities can be calculated:

$$n_{op} = \frac{220\ \text{day/year} \times 16\ \text{h/day} \times 3600\ \text{s/h}}{5\ \text{s/cycle}} = 2{,}53 \times 10^6\ \text{cycles/year} \quad \text{(C.8)}$$

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

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

This will give a $MTTF_D$ for the component "high" according to Table 5. These assumptions are only valid for a restricted operation time of 23,7 years for the valve.

C.5 $MTTF_D$ data of electrical components

C.5.1 General

Tables C.2 to C.7 indicate some typical average values of $MTTF_D$ for electronic components. The data are extracted from the SN 29500 series database.[46] All data are of general type. Various databases 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 highly recommended.

The values given in Tables C.2 to C.7 are valid for a temperature of 40 °C, nominal load for current and voltage.

In the MTTF column of the tables, the values from SN 29500 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 Tables C.2 and 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_{tot} < 1 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 Tables C.4 to 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

Table C.4 *(continued)*

Capacitor	Example	MTTF for components years	$MTTF_D$ for components years Typical	Remark
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	7 618	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.[3)]

The general formula is

$$\frac{1}{MTTF_D} = \sum_{i=1}^{\tilde{N}} \frac{1}{MTTF_{D\,i}} = \sum_{j=1}^{\tilde{N}} \frac{n_j}{MTTF_{D\,j}} \qquad (D.1)$$

where

$MTTF_D$ is for the complete channel;

$MTTF_{D\,i}$ / $MTTF_{D\,j}$ is the $MTTF_D$ of each component which has a contribution to the safety 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 Table 5.

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

j	Component	Units n_j	$MTTF_{D\,j}$ typical years	$1/MTTF_{D\,j}$ typical 1/year	$n_j/MTTF_{D\,j}$ typical 1/year
1	Transistors, bipolar, low power (see Table C.2)	2	11 416	0,000 087 6	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
$\sum(n_j / MTTF_{D\,j})$					0,044 548 0
$MTTF_D = 1 / \sum(n_j / MTTF_{D\,j})$ [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.

3) The *parts count method* is an approximation which always errs on the safe side. If more exact values are required, the designer should take the failure modes into account, but this can be very complicated.

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} will lead to a much better result, that is, a higher $MTTF_D$ for the channel.

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

The designated architectures of 6.2 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 5.

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:

$$MTTF_D = \frac{2}{3}\left[MTTF_{D\,C1} + MTTF_{D\,C2} - \frac{1}{\frac{1}{MTTF_{DC1}} + \frac{1}{MTTF_{DC2}}}\right] \quad \text{(D.2)}$$

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) before Formula D.2 is applied.

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 5.

NOTE This method assumes independent parallel channels.

Annex E
(informative)

Estimates for diagnostic coverage (DC) for functions and modules

E.1 Examples of diagnostic coverage (DC)

See Table E.1

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

Measure	DC
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	0 % to 99 %, depending on how often a signal change is done by the application
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 actuators)	90 % to 99 %, depending on the application
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	0 % to 99 %, depending on the application; this measure alone is not sufficient for the required performance level e!
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 actuators)	90 % to 99 %, depending on the application
Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99 %
Simple temporal time monitoring of the logic (e.g. timer as watchdog, where trigger points are within the program of the logic)	60 %
NOTE 1 For additional estimations for DC, see, e.g. IEC 61508–2:2010, Tables A.2 to A.15.	
NOTE 2 If medium or high DC is claimed for the logic, at least one measure for variable memory, invariable memory and processing unit with each DC at least 60 % has to be applied. There may also be measures that used other than those listed in this table.	
NOTE 3 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.	

Table E.1 *(continued)*

Measure	DC
Temporal and logical monitoring of the logic by the watchdog, where the test equipment does plausibility checks of the behaviour of the logic	90 %
Start-up self-tests to detect latent faults in parts of the logic (e.g. program and data memories, input/output ports, interfaces)	90 % (depending on the testing technique)
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 (8 bit)	90 %
Invariable memory: signature of double word (16 bit)	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 monitoring with modified Hamming code or RAM self-test (e.g. “galpat” or “Abraham”)	99 %
Processing unit: self-test by software	60 % to 90 %
Processing unit: coded processing	90 % to 99 %
Fault detection by the process	0 % to 99 %, depending on the application; this measure alone is not sufficient for the required performance level “e”!
Output device	
Monitoring of outputs by one channel without dynamic test	0 % to 99 % depending on how often a signal change is done by the application
Cross monitoring of outputs without dynamic test	0 % to 99 % depending on how often a signal change is done by the application
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 actuators by logic and test equipment	99 %
Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90 % to 99 %, depending on the application
Fault detection by the process	0 % to 99 %, depending on the application; this measure alone is not sufficient for the required performance level “e”!
NOTE 1 For additional estimations for DC, see, e.g. IEC 61508–2:2010, Tables A.2 to A.15.	
NOTE 2 If medium or high DC is claimed for the logic, at least one measure for variable memory, invariable memory and processing unit with each DC at least 60 % has to be applied. There may also be measures that used other than those listed in this table.	
NOTE 3 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.	

Table E.1 *(continued)*

Measure	DC
Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99 %
NOTE 1 For additional estimations for DC, see, e.g. IEC 61508–2:2010, Tables A.2 to A.15. NOTE 2 If medium or high DC is claimed for the logic, at least one measure for variable memory, invariable memory and processing unit with each DC at least 60 % has to be applied. There may also be measures that used other than those listed in this table. NOTE 3 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.	

For the application of Table E.1 see the indicative examples below.

EXAMPLE 1 Annex E of ISO 13949-2 presents a complete worked example (which is very detailed) for the validation of fault behaviour and diagnostic means on an automatic assembly machine.

EXAMPLE 2 ISO/TR 24119 describes a pragmatic step-by-step table based methodology for evaluation of diagnostic coverage for series connected interlocking devices.

EXAMPLE 3 The DC measure "fault detection by the process" may 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 redundant functional channels executing the safety function. The appropriate DC level depends on the overlap of the commonly used resources (logic, inputs/outputs etc.). E.g. 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 may be estimated as 90 % up to 99 %.

E.2 Estimation of average DC (DC_{avg})

In many systems, several measures for fault detection might be used. These measures could check different parts of the SRP/CS and have different DC. For an estimation of the PL according to Figure 5 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 the following formula:

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

Here all components of the SRP/CS without fault exclusion have to 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)

Estimates for common cause failure (CCF)

F.1 Requirements for CCF

A comprehensive procedure for measures against CCF for sensors/actuators and separately for control logic is given, for example, in IEC 61508-6:2000, Annex D. Not all measures given therein are applicable to machinery. The most important measures are given here.

NOTE In this part of ISO 13849, it is assumed that for redundant systems a β-factor according to IEC 61508–6:2000, Annex D should be less than or equal to 2 %.

F.2 Estimation of effect of CCF

This quantitative process should be passed for the whole system. Every part of the safety-related parts of the control system should be considered.

Table F.1 lists the measures and contains associated values, based on engineering judgement, which represent the contribution each measure makes in the reduction of common cause failures.

For each listed measure, only the full score or nothing can be claimed. If a measure is only partly fulfilled, the score according to this measure is zero.

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

No.	Measure against CCF	Score
1	**Separation/ Segregation**	
	Physical separation between signal paths, for example: — separation in wiring/piping; — detection of short circuits and open circuits in cables by dynamic test; — separate shielding for the signal path of each channel; — sufficient clearances and creepage distances on printed-circuit boards.	**15**
2	**Diversity**	
	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), and/or digital and analog measurement of variables (e.g. distance, pressure or temperature) and/or Components of different manufactures.	**20**
a Where technological measures are not relevant, points attached to this column can be considered in the comprehensive calculation.		

Table F.1 *(continued)*

No.	Measure against CCF	Score
3	**Design/application/experience**	
3.1	Protection against over-voltage, over-pressure, over-current, over-temperature, etc.	**15**
3.2	Components used are well-tried.	**5**
4	**Assessment/analysis**	
	For each part of safety related parts of control system a failure mode and effect analysis has been carried out and its results taken into account to avoid common-cause-failures in the design.	**5**
5	**Competence/training**	
	Training of designers to understand the causes and consequences of common cause failures.	**5**
6	**Environmental**	
6.1	For electrical/electronic systems, prevention of contamination and electromagnetic disturbances (EMC) to protect against common cause failures in accordance with appropriate standards (e.g. IEC 61326–3-1). Fluidic systems: filtration of the pressure medium, prevention of dirt intake, drainage of compressed air, e.g. in compliance with the component manufacturers' requirements concerning purity of the pressure medium. NOTE For combined fluidic and electric systems, both aspects should be considered.	**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).	**10**
	Total	**[max. achievable 100]**

Total score	**Measures for avoiding CCF[a]**
65 or better	Meets the requirements
Less than 65	Process failed ⇒ choose additional measures

[a] Where technological measures are not relevant, points attached to this column can be considered in the comprehensive calculation.

Annex G
(informative)

Systematic failure

G.1 General

ISO 13849-2 gives a comprehensive list of measures against systematic failure which should be applied, such as basic and well-tried safety principles.

G.2 Measures for the control of systematic failures

The following measures should be applied.

— Use of de-energization (see ISO 13849-2)

The safety-related parts of the control system (SRP/CS) should be designed so that with loss of its power supply a safe state of the machine can be achieved or maintained.

— 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 and IEC 61508-7:2000, A.8).

— Measures for controlling or avoiding the effects of the physical environment (for example, temperature, humidity, water, vibration, dust, corrosive substances, electromagnetic interference 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).

— Program sequence monitoring shall be used with SRP/CS containing software in order 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 EN 61508-7:2001, A.9).

— Measures for controlling the effects of errors and other effects arising from any data communication process (see IEC 61508-2:2000, 7.4.8)

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 derating will improve reliability — where over-dimensioning is appropriate, an over-dimensioning factor of at least 1,5 should be used.

See also ISO 13849-2:2012, D.3.

G.3 Measures for avoidance of systematic failures

The following measures should be applied.

— 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.

— Correct dimensioning and shaping

Consideration of, e.g. stress, strain, fatigue, temperature, surface roughness, tolerances, manufacturing.

— 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.

— Compatibility

Use components with compatible operating characteristics.

NOTE 1 Components such as hydraulic or pneumatic valves can require cyclic switching to avoid failure by non-switching or unacceptable increase in switching times. In this case a periodic test is necessary.

— 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 electromagnetic interference (EMI) (see ISO 13849-2:2012, D.2).

— 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 61508-7:2000, 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 (see IEC 61508-7:2000, B.3.7 and B.3.8).

— 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 (see IEC 61508-7:2000, B.3.5).

— 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 (see IEC 61508-7:2000, B.3.6).

NOTE 2 IEC 61508–2:2010, Annex F specifies techniques and measures for avoidance of systematic failures during design and development of application-specific integrated circuits (ASICs), field programmable gate arrays (FPGAs), programmable logic devices (PLDs) etc.

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.

Annex H
(informative)

Example of combination of several safety-related partsof the control system

Figure H.1 is a schematic diagram of the safety-related parts providing one of the 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 valve. The risk is reduced by a AOPD, which detects access to the hazardous situation and prevents start-up of the fluidic actuator when the light beam is interrupted.

The safety-related parts which provide the safety function are: AOPD, electronic control logic, hydraulic directional valve and the interconnecting means.

These combined safety-related parts 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 valve to stop the hydraulic flow as the output of the SRP/CS. At the machine, this stops the hazardous movement of the actuator.

This combination of safety-related parts 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 part of ISO 13849, the safety-related parts shown in Figure H.2 can be described as follows.

— Category 2, PL = c for the electro-sensitive protective device (light barrier). To reduce the probability of faults this device uses well-tried safety principles;

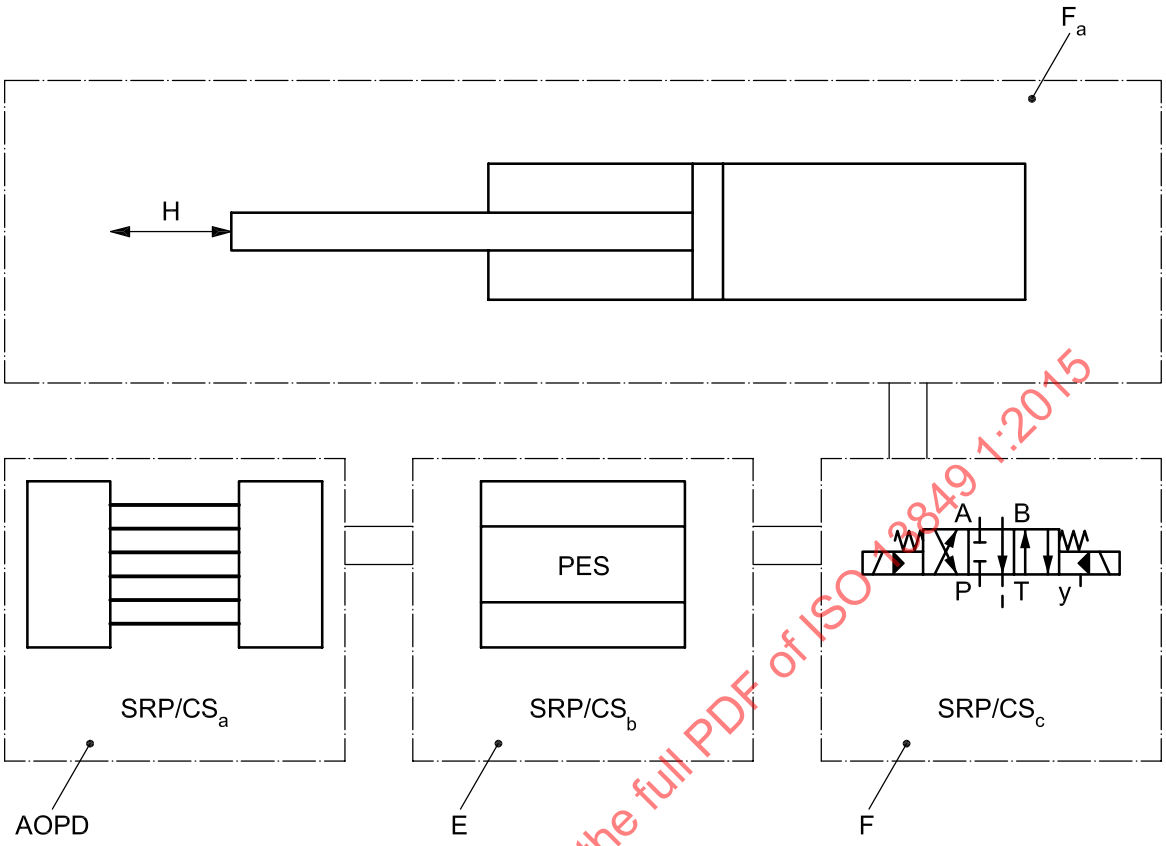
— Category 3, PL = d for the electronic control logic. To increase the level of safety performance of this electronic control logic, the structure of this SRP/CS is redundant and implements several fault detection measures such that it is able to detect most of single faults;

— Category 1, PL = c for the hydraulic directional 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 6.2.4).

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

This combination leads with PL_{low} = c and N_{low} = 2 to an overall performance level pf PL = c (see 6.3).

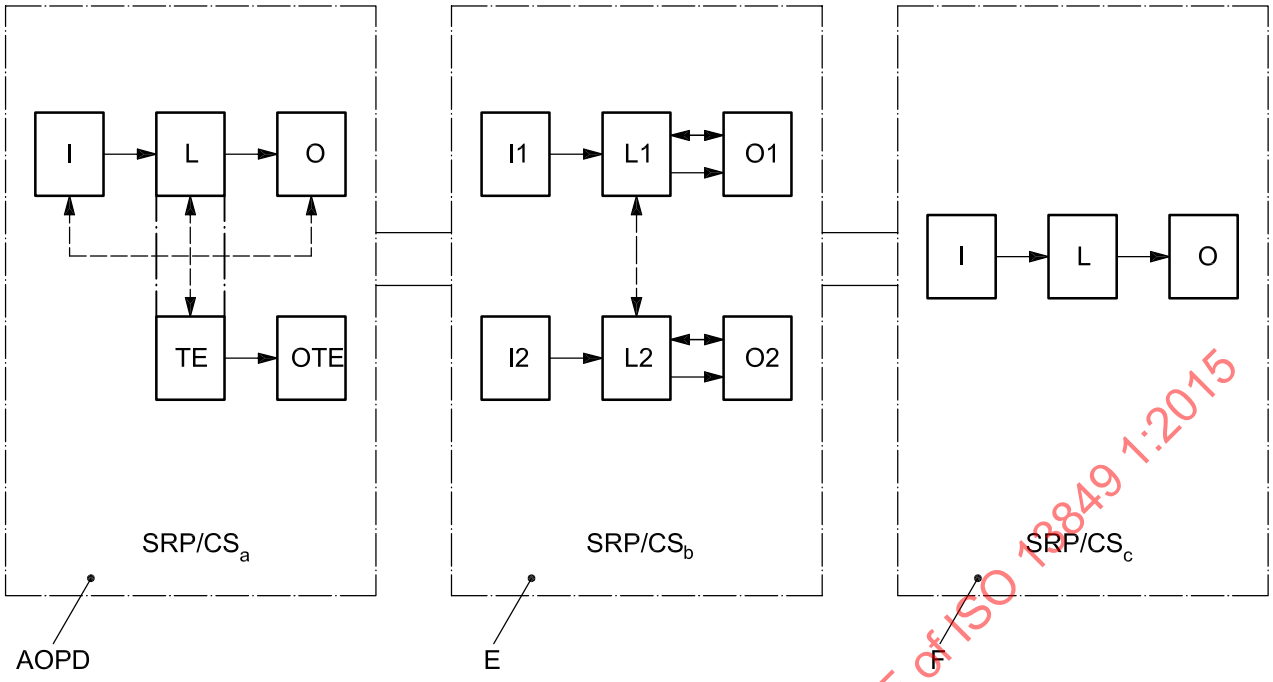
NOTE 2 In case of one fault in the category 1 or the category 2 parts of Figure H.2 there may be a loss of the safety function.



Key

AOPD	active optoelectronic protective device (e.g. light barrier), SRP/CS_a: Category 2 [Type 2], PL = c
E	electronic control logic, SRP/CS_b: Category 3, PL = d
F	fluidics, SRP/CS_c: Category 1, PL = c
F_a	fluidic actuator
H	hazardous movement

Figure H.1 — Example — Block diagram explaining combination of SRP/CS



Key

AOPD	active optoelectronic protective device (e.g. light barrier)
E	electronic control logic
F	fluidics,
I, I1, I2	input devices, e.g. sensor
L, L1, L2	logic
O, O1, O_2, OTE	output devices, e.g. main contactor
TE	test equipment

Figure H.2 — Substitution of Figure H.1 by designated architectures