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.

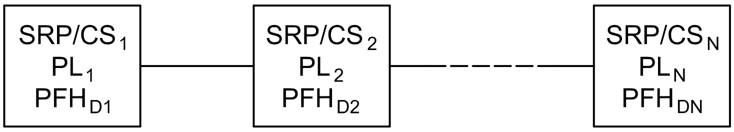
It is assumed that there are N separate SRP/CS$_i$ in a series combination, which as a whole performs a safety function. For each SRP/CS$_i$, a PL$_i$ has already been evaluated. This situation is illustrated in Figure 13 (see also Figure 4 and Figure H.2).

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

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

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 ($\mathrm{MTTF_D}$, 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 ($\mathrm{PL_r}$)

A.1 Selection of $\mathrm{PL_r}$

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 $\mathrm{PL_r}$ for each necessary safety function to be carried out by an SRP/CS.

NOTE This methodology to estimate the $\mathrm{PL_r}$ 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

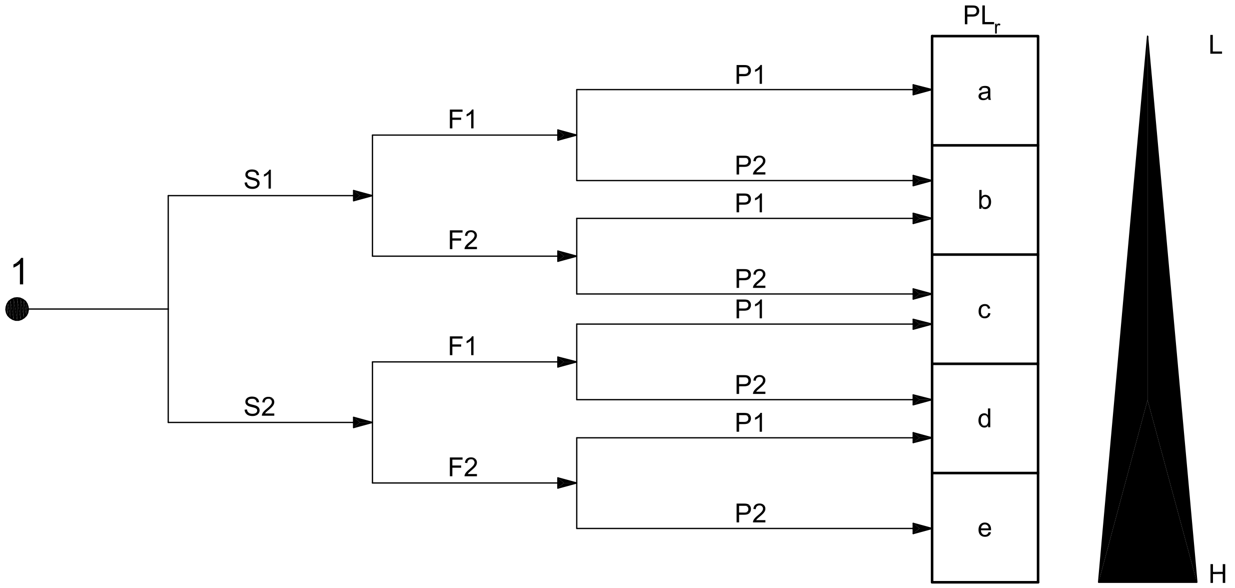
The probability of occurrence of a hazardous event depends on either human behaviour or technical failures. In most cases, the appropriate probabilities are unknown or hard to identify. The estimation of the probability of occurrence of a hazardous event should be based on factors including:

- 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 $\mathrm{MTTF_D}$ of the block based on the $\mathrm{MTTF_D}$ 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.

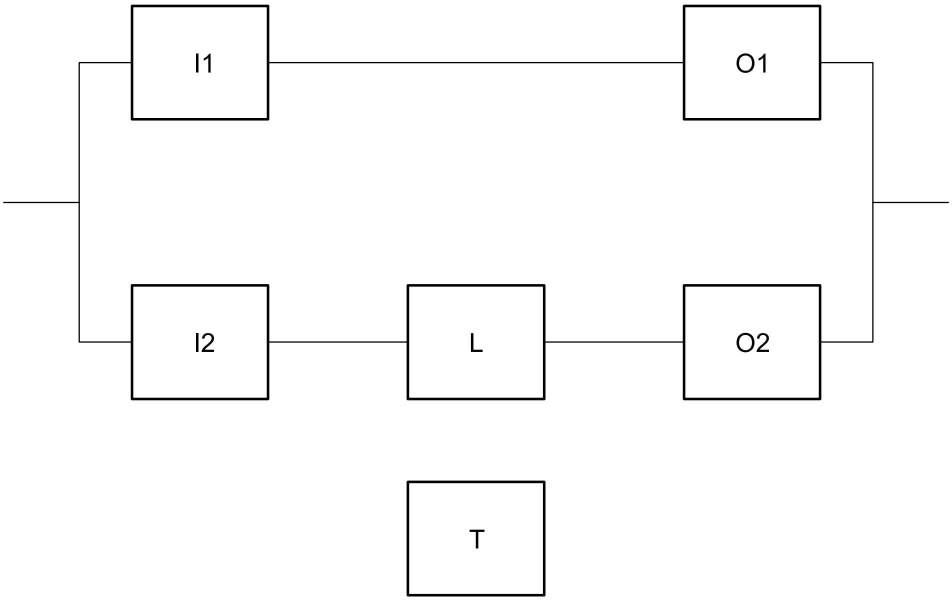
NOTE For the purposes of this part of ISO 13849, “blocks” do not correspond to functional blocks or reliability blocks.

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 $\mathrm{MTTF_D}$ values for single components

C.1 General

Annex C gives several methods for calculating or evaluating $\mathrm{MTTF_D}$ 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 $\mathrm{MTTF_D}$ of pneumatic, mechanical and electromechanical components from B_{10} (see C.4.1); C.5 lists $\mathrm{MTTF_D}$ values for electrical components.

C.2 Good engineering practices method

If the following criteria are met, the $\mathrm{MTTF_D}$ or $B_{10\mathrm{D}}$ 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 $\mathrm{MTTF_D}$ 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 $\mathrm{MTTF_D}$ 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 $\mathrm{MTTF_D}$ value can be estimated higher as shown in Table C.1

But if either a) or b) is not achieved, the $\mathrm{MTTF_D}$ value for the single hydraulic component has to be given by the manufacturer. Instead of using a fixed value for the $\mathrm{MTTF_D}$ as described above it is permissible to use the $\mathrm{B_{10D}}$-concept for $\mathrm{MTTF_D}$ of pneumatic, mechanical and electromechanical components also for hydraulic components if the manufacturer can provide data.