Approaching standard by designing a basic safety function

James Baudoin, Jean-Paul Bello

Institut National de Recherche et de Sécurité

Approaching standard EN ISO 13849-1 by designing a basic safety function

NS 315 NOTE SCIENTIFIQUE ET TECHNIQUE

Approaching standard EN ISO 13849-1 by designing a basic safety function

James Baudoin
Jean-Paul Bello

INRS, Work Equipment Engineering Department
Safety of Automated Systems Laboratory

NS 315
janvier 2014

Institut national de recherche et de sécurité pour la prévention des accidents du travail et des maladies professionnelles
Siège social : 65, boulevard Richard-Lenoir 75011 Paris • Tél. 01 40 44 30 00
Centre de Lorraine : 1, rue du Morvan CS 60027 54519 Vandœuvre-les-Nancy cedex • Tél. 03 83 50 20 00

Abstract:

This document is intended to guide designers to perform machinery control systems with only one or a few "basic" safety functions such as emergency stop or movable guard.

Among the available standards for machine design, EN ISO 13849-1 is the one providing recommendations to design safety related parts of control systems (SRP/CS) implementing different types of energy such as electric, hydraulic or pneumatic.

This document is based on the implementation of the simplified method of EN ISO 13849-1 and helps to understand the new concepts introduced by this standard.

The first part of the document entitled: Design guide for a SRP/CS, sheds light on some parts of the standard and also provides tools (graphs, tables ...) to facilitate the understanding and use but also choices that designers will have to do.

The second part consists of a practical case of a safety function designed by INRS using the standard and the tools shown in the guide. All phases of design are discussed, highlighting details and comments deemed necessary to assimilate the principles advocated by the standard.

Although new, the standard EN ISO 13849-1 does not bring major changes in the design of control systems related to safety. It retains much of the design principles recommended in the standard EN 954-1 that it replaces. The main new of this framework lies in the quantification of a number of parameters.

This document is a translation into English of NS 302 first issue in French dated February 2013.

TABLE OF CONTENTS

Foreword

During the design of working equipment, such as a machine, it is necessary to take its "control system" into account. The control system is designed to ensure that the equipment functions as expected. When safety functions are necessary, the control system must also treat them to reduce the risks related to using the equipment, both for operators and exposed third parties.

Among the available reference texts for machine design, standard EN ISO 13849-1[1] can be used to develop control systems relying on various types of energy, including electric, hydraulic and pneumatic. This standard describes the general principles for the design of safety-related parts of control systems (SRP/CS).

EN ISO 13849-1 replaces standard EN 954-1[2] which was widely used in industry, but is no longer valid.

The new standard does not make many significant changes to the design of control systems with regards to safety as it retains the majority of the design principles recommended in standard EN 954-1. For example, the designer must continue to implement:

- components appropriate for the function for which they are destined,
- components designed according to proven safety principles,
- single- or double-channel architectures (redundancy),
- where necessary, diagnostic procedures to test the components (self-checking),
- means to avoid systematic failures.

The main novelty in this reference text is the quantification of a certain number of parameters, including:

- calculation of the $MTTF_d$ (Mean Time To dangerous Failure) from data relating to reliability and solicitation of the components implemented,
- quantification of the measures to ensure diagnostic coverage for the components,
- quantification of measures to avoid common cause failures.

Contrary to what might be expected, these calculations are straightforward and limited if the simplified procedure described in the standard is used, and particularly when the safety functions to be designed are simple and involve few components, or when the selected components have known performance levels.

In the case of more complex applications, a software tool is freely available: SISTEMA. It assists the designer in applying EN ISO 13849-1 by taking them through the different design phases recommended by the standard and by calculating the necessary data without requiring external recourse to the formulae.

This document aims to guide SRP/CS designers in the use of the standard and to help them understand the new ideas that it introduces. It is based on a practical case treated by INRS.

Warning 1

This document is in no case a substitute for the standard which should be read first and used throughout the design process. This is important as not all of the recommendations from the standard are mentioned here.

Note: In the remainder of this document, all references (paragraph, table, etc.), unless specified, refer to the present document.

[1] EN ISO 13849-1: 2008: Safety of machinery. Safety-related parts of control systems - Part 1: General principles for design (called "**the standard**" in the document)
[2] EN 954-1: 1997: Safety of machinery. Safety-related parts of control systems - Part 1: General principles for design

Guide to designing an SRP/CS

1 Introduction

This document is intended as a guide to designers developing SRP/CS, it is based on the simplified method described in EN ISO 13849-1 (see § 4.5.4 of the standard), but does not address the related software (§ 4.6 and Annex J of the standard), or the validation phase (§ 8 of the standard, which refers to standard EN ISO 13849-2[3] in particular).

The system controlling the safety features of a machine is composed of one or more safety functions. A specific part of the control system is dedicated to each safety function. To facilitate reading, this is abbreviated as (SF/CS[4] in the remainder of this guide).

Each SF/CS includes at least one material part (SRP/CS) and may also include a software part. A SF/CS must conform to a defined performance level appropriate for the safety function it performs.

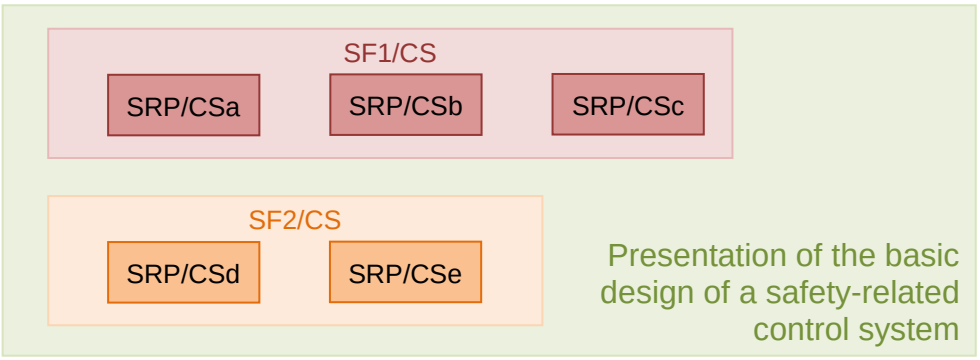


Figure 1: Sample structure of a safety-related control system of a machine

2 Specification of a safety function

The first step in designing a SF/CS is to precisely define the safety function that it will perform, in particular by describing the following:

- its required safety performance level, PL_r (see § 3),
- its activation conditions, such as the operating modes in which the function is active/inactive,
- how it works, describing the expected action, as a function of the input information,
- its level of priority relative to other simultaneous functions,
- its maximum reaction time,
- Its frequency of solicitation,
- environmental conditions,
- etc.

3 Determination of the required performance level

A SF/CS must perform to a certain level to be able to ensure the safety function it is designed to control. In EN ISO 13849-1, the capacity of a SF/CS to perform a safety function is expressed by determining its performance level (PL). The standard defines 5 possible performance levels for a control system, from PL "a" to PL "e" (see Figure 2). Before designing a SF/CS, it is essential to determine the required performance level (PL_r) for the safety function. The PL achieved by the SF/CS must be at least equal to the PL_r for this safety function. The PL_r

[3] EN ISO 13849-2: 2008: Safety of machinery. Safety-related parts of control systems – Part 2: Validation
[4] SF/CS: Control System of the Safety Function (this abbreviation is not standardised).

depends on how much the safety function contributes to risk reduction, which is determined based on an estimation of this risk. Annex A of the standard provides a method to determine the PL_r.

The PL_r for each SRP/CS composing a SF/CS must be at least equal to the PL_r of this SF/CS.

For each performance level, the standard provides an equivalent average probability of dangerous failure per hour (PFH_d) for the control system (Table 3 of the standard). A failure is termed dangerous when it could lead to a potentially dangerous situation.

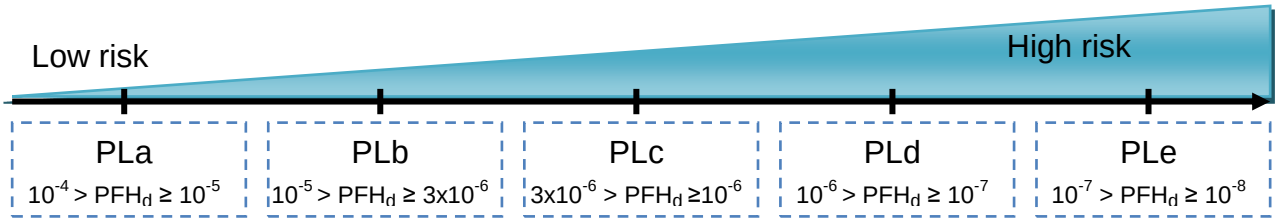


Figure 2

4 General design process for a SF/CS

4.1 General logical structure model for a SF/CS

A SF/CS generally includes several logical entities to treat the input orders and to control pre-actuators through a Logic unit. Figure 3 represents the most common construction, composed of three elements.

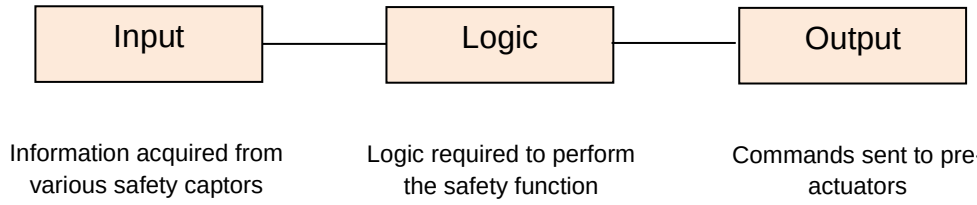


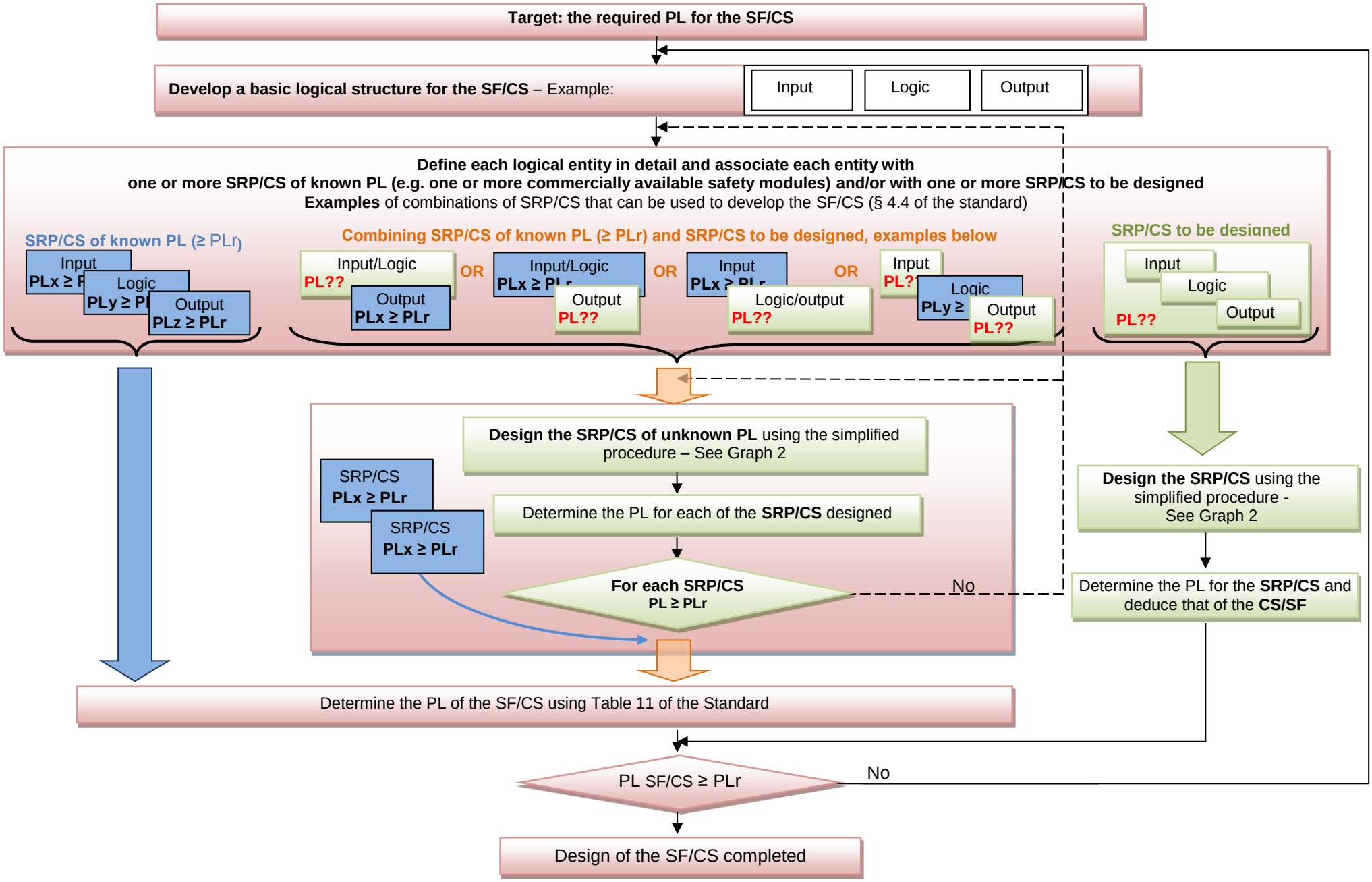
Figure 3

The designer can choose to develop these logical entities as one or more SRP/CS depending on the material he/she expects to use. This development can be done in different ways, as illustrated in paragraph 4.2.

4.2 Graph of the general design process for a SF/CS conforming to a required PL

Graph 1 illustrates:

- various design pathways suggested by EN ISO 13849. The designer's choice is determined by the commercially available components, by the specific design practices for each company, by the complexity of the SF/CS to be developed, by the technology behind the components used, etc.
- various means to determine the performance level "PL" achieved by a SF/CS, and to compare it to the required PL.



Graph 1: General design process for a SF/CS conforming to a required PL

Guide to designing an SRP/CS

Graph 1 shows that the designer of a control system has three options:

- In the left branch, he/she only combines SRP/CS of known PL (data provided by the manufacturer) greater than or equal to the required PL for the SF/CS (represented in blue). Examples are: a commercially available safety logic unit, a light curtain, etc. (example Figure 4). The PL of the SF/CS is determined by applying paragraph 6.3 of the standard, in particular Table 11 (Take Warning 2 of this document into account).

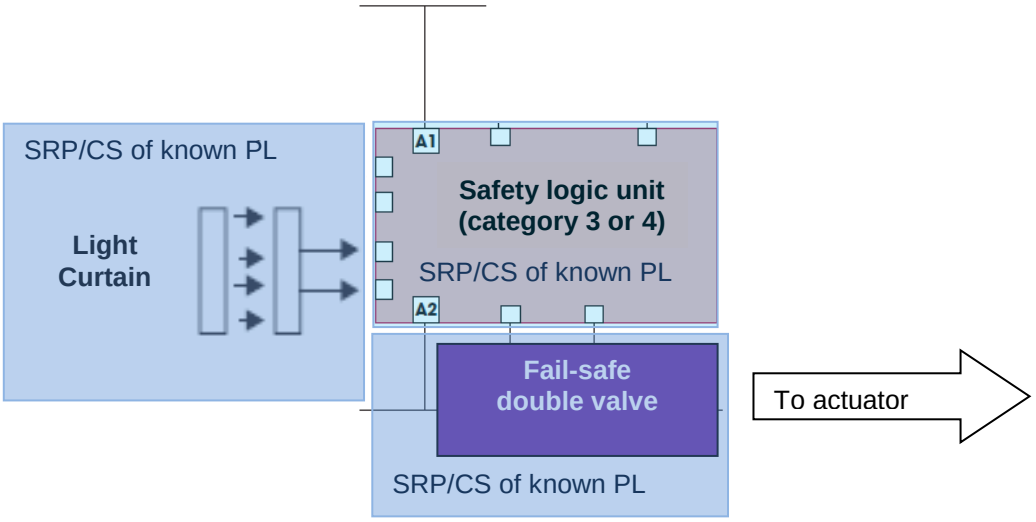


Figure 4: Example of a SF/CS composed of 3 SRP/CS of known PL

- In the central branch, a mixed solution is illustrated. The designer combines one or more SRP/CS of known PL, greater than or equal to the required PL for the SF/CS (represented in blue) and one or more SRP/CS of his/her own design (represented in green), an example is given in Figure 5. The steps in designing an SRP/CS are presented in Graph 2: Details of the design of an SRP/CS to achieve a required PL .
  The PL of the SF/CS is determined by applying paragraph 6.3 of the standard, in particular Table 11 (Take Warning 2 of this document into account).

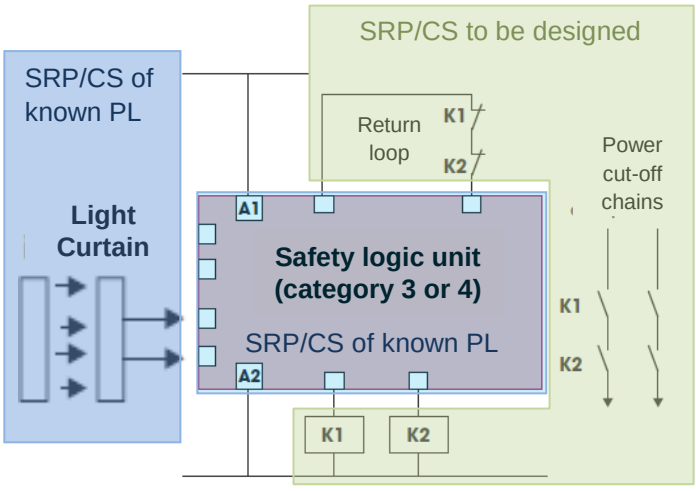


Figure 5: Example of an SF/CS combining SRP/CS of known PL with an SRP/CS to be designed

- In the right-hand branch, the designer uses a single SRP/CS of his/her own design (represented in green) (see Figure 6).
  This could, for example, involve assembling basic components, such as position switches, proximity sensors and electromechanical relays.
  The steps in designing a SRP/CS are presented in Graph 2: Details of the design of an SRP/CS to achieve a required PL .

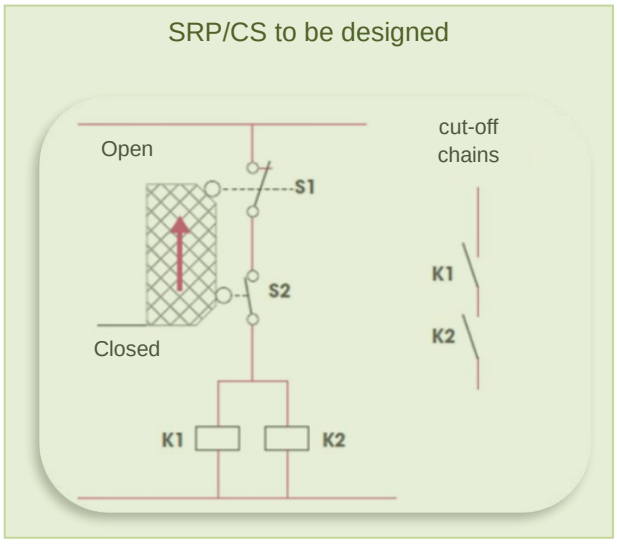


Figure 6: Example of a SF/CS composed of a single SRP/CS to be designed

Warning 2

Combining several SRP/CS within a single SF/CS

When combining several SRP/CS in series[5], the PL achieved by each one must be determined. The PL of the SF/CS as a whole will depend on that of the SRP/CS it is composed of. It will thus be:

- Equal to the lowest PL for the different SRP/CS if only one SRP/CS has achieved this PL.
  Example

- Lower than or equal to the lowest PL, depending on the number of SRP/CS having achieved this PL. Table 11 in the standard indicates the overall PL as a function of the number of SRP/CS with the lowest PL.
  In the following example, the lowest PL is "PLe". If more than three SRP/CS have a PLe, Table 11 of the standard indicates that the PL of the SF/CS is "PLd".

[5] In series: implementation of several SRP/CS such that failure of any single SRP/CS leads to failure of the whole CS/SF

4.3 Specifications of an SRP/CS

Depending on the design strategy selected, each of the SRP/CS making up the SF/CS will either be chosen "off the shelf", or specifically designed. In either case, it is necessary to specify, based on the specifications of the SF/CS in which it will be integrated (see paragraph 2), the function the SRP/CS is to perform, in particular by determining:

- its required PL, which should be at least equal to the PL_r of the SF/CS,
- its activation conditions, such as the operating modes in which the SRP/CS is active/inactive,
- how it works, describing the expected action, as a function of the input information,
- its interaction with the other SRP/CS making up the SF/CS,
- its level of priority relative to other simultaneous functions,
- its maximum reaction time,
- how often it will be solicited (which can differ for the SF/CS),
- environmental conditions,
- etc.

Note: when a SF/CS consists of a single SRP/CS, the specifications for the SRP/CS are identical to those of the safety function and there is no need to formulate a new specification.

5 Combining SRP/CS of known PL

When a SF/CS is produced by combining (e.g. Figure 4) or integrating (e.g. Figure 5) SPR/CS of known PL, it is also necessary to implement measures to avoid systematic failures. This mainly means conforming to the instructions relating to the various components and to inter-component connections (see the example in Figure 17, paragraph A5.2).

6 Details of designing an SRP/CS

6.1 Principle

For each SRP/CS to be designed, the designer's will aim to implement the measures necessary to achieve a performance level at least equal to the PL_r for the SF/CS. To do this, it is essential to consider the following criteria, which are listed in § 4.5.1 of the standard:

- the structure (see Clause 6 of the standard),
- the behaviour of the safety function under fault conditions (see Clause 6 of the standard),
- the ability to perform a safety function in the expected environmental conditions,
- common cause failures (CCF) (see Annex F of the standard),
- systematic failures (see Annex G of the standard),
- the $MTTF_d$ (mean time to dangerous failure) for individual components (see Annexes C and D of the standard),
- the diagnostic coverage (DC) (see § 4.5.3 and Annex E of the standard),
- the safety-related software (see § 4.6 and Annex J of the standard).

6.2 Recommendations for selecting the most appropriate minimal requirements when designing an SRP/CS

At the start of SRP/CS design, the presentation used in the standard makes it difficult to have an overall view of the various ways in which the PL_r and the minimal required criteria can be met. For example, what authorised categories, or target $MTTF_d$ values should be aimed for?

To provide this overview and facilitate choices, tables are presented in this document (see Annex 1). These tables are mainly based on Table 7 of the standard and are destined for use as part of the simplified procedure suggested to achieve the required PL.

Five tables are provided, each one corresponding to one of the five PL_r levels (a, b, c, d and e) to which an SRP/CS can conform. Each column of the tables presents the categories of components which may be implemented to achieve the PL_r, and minimal recommendations are made (designated architecture, $MTTF_d$, DC_{avg}, CCF, etc.).

These tables give an overview of what is necessary when designing an SRP/CS to a given PL_r, and thus make it possible to anticipate material choices (e.g. $MTTF_d$) to achieve the required minimal criteria.

When designing an SRP/CS with a given PL_r, it is thus necessary to select the appropriate table and to choose a column corresponding to one of the four categories. The choice of column can be guided by the designer's experience or by the characteristics of the available components likely to meet the criteria listed in the column. If the design cannot be completed, it may be necessary to repeat the selection process, using a different column in the same table.

Note: The $MTTF_d$ ranges for each channel and the DC ranges listed in these tables are those presented in the standard, they are expressed in a format to facilitate their use. Indeed, the standard presents minimal values which must be respected. If the results of $MTTF_d$ or DC_{avg} calculations are greater than the recommended values, they can also appropriate, as clearly shown in these tables.

Ranges defined in the standard: $MTTF_d$ by channel (Table 5) and DC (Table 6)

$MTTF_d$ (by channel)
Low $MTTF_d$: 3 years ≤ $MTTF_d$ < 10 years
Medium $MTTF_d$: 10 years ≤ $MTTF_d$ < 30 years
High $MTTF_d$: 30 years ≤ $MTTF_d$ ≤ 100 years

DC
Null: DC < 60%
Low: 60% ≤ DC < 90%
Medium: 90% ≤ DC < 99%
High: 99% ≤ DC

Reflections on the criteria relating to category 2
(If the simplified procedure is used to calculate $MTTF_d$)

To meet the criteria for category 2 systems, the standard requires, in particular, that the test rate for the part considered be at least 100-fold its demand rate (§ 3.1.30 of the standard - frequency of demands for a safety-related action of the SRP/CS).

In practice, this requirement almost always makes it impossible to use electromechanical, pneumatic or hydraulic components which do not commute. Because of this, their test rate is equivalent to their demand rate, except in very rare cases where it would be possible:

- to "artificially" control (other than by triggering the safety function through its input element) commutation of the electromechanical components of the SF/CS at a rate 100-fold greater than its demand rate,
- that this commutation, for testing purposes, does not affect the normal operation of the machine.

With a position switch with electromechanical contacts activated by a guard, there is no way to "artificially" activate the switch for testing purposes. There is thus no way to generate a test rate greater than the demand rate.

Use of category 2 is therefore mainly restricted to electronic systems, which can tolerate enough test micro-pulses to perform frequent diagnostic tests, without affecting the output of the system tested with regard to elements controlled by the system.

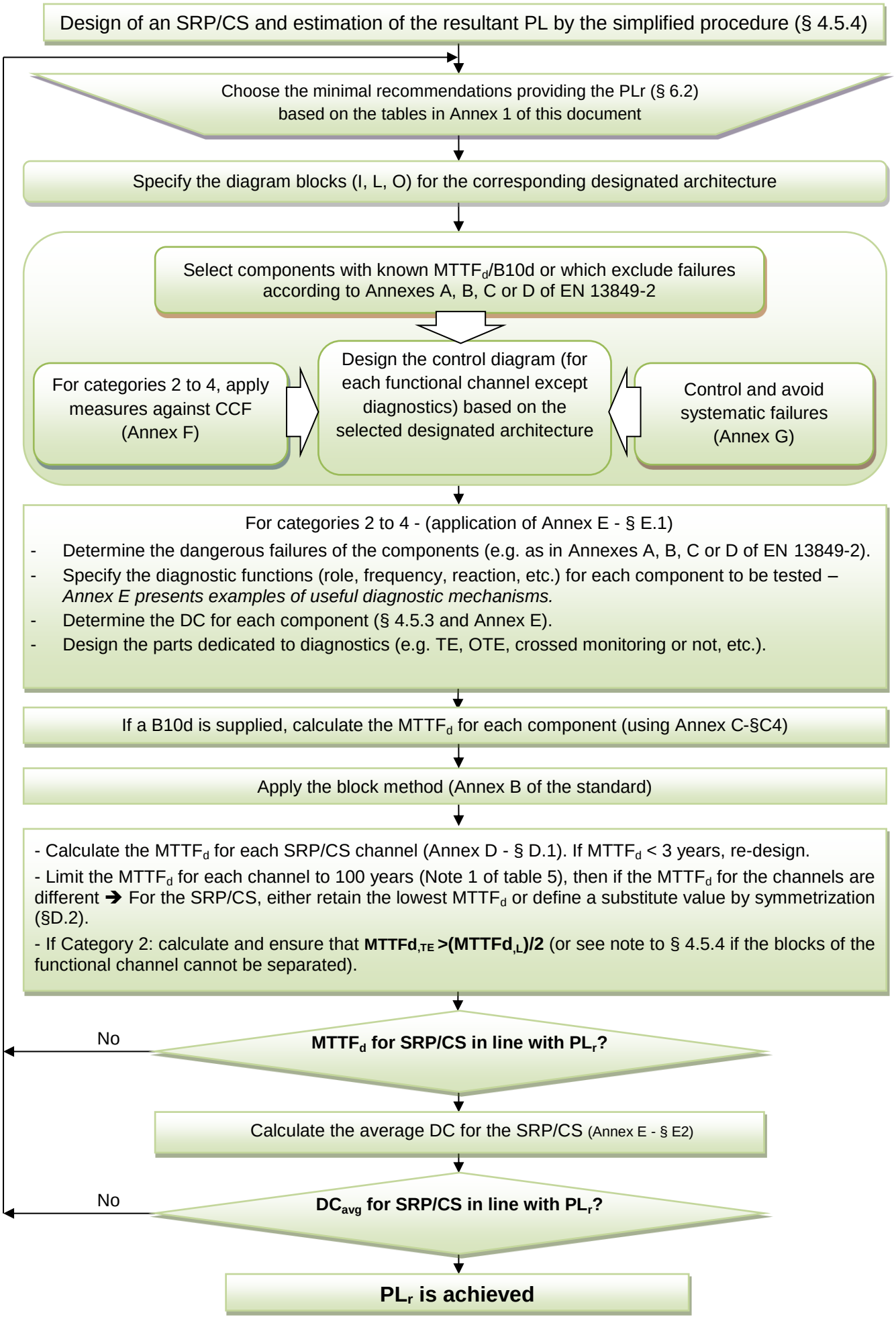
Consequently, when an SRP/CS is to be developed using electromechanical, pneumatic or hydraulic components, it is strongly recommended to avoid using a category 2 architecture. It is better to use another category appropriate for the PL_r.

6.3 Steps in designing an SRP/CS

To facilitate the design of an SRP/CS (apart from its software elements) using the simplified method described by the standard, Graph 2 was developed.

Reminder: the simplified method is based on designated architectures for which "pre-calculations" have been performed, this facilitates application of the standard's quantitative requirements.

The graph lists and ranks the steps to be followed and indicates the different paragraphs or Annexes of EN ISO 13849-1 which the reader should consult.



Graph 2: Details of the design of an SRP/CS to achieve a required PL

Guide to designing an SRP/CS

6.4 Taking systematic failures into account

Reminder: *systematic failure (§ 3.1.7 of the standard)*

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.

Many designers fail to take systematic failures into account, preferring more readily calculable parameters, such as $MTTF_d$. However, without appropriate means to overcome these failures, a control system will not be able to achieve an appropriate working level of safety. How should a safety-related control system be viewed if its behaviour is affected simply by accidentally earthing one of its parts?

These points are mainly requirements for electrical control circuits, but when hydraulic or pneumatic energy is used to run a machine, the same design, safe conditions objectives should be achieved by applying appropriate measures.

For the sample SF/CS design treated in this document, the measures to implement and a reminder of the recommendations in the standard are supplied in table format (see Table 20). These measures are based either:

- on "basic safety principles" and "well-tried safety principles" from Tables A1 and A2, B1 and B2, C1 and C2 or D1 and D2 in Annexes A, B, C and D of standard ISO 13849-2, depending on the technology applied,
- or on the methods currently applied in industry.

When an SRP/CS is made up of several parts (e.g. an input "I", a logic "L" and an output "O"), the requirements of each of these parts must be considered.

6.5 Requirements to assess measures to prevent common cause failures (CCF)

Reminder: *common cause failures CCF (§ 3.1.6 in the standard)*

Failures of different items, resulting from a single event, where these failures are not consequences of each other.

Note: As indicated in § 6.2.5 to 6.2.7 of the standard, common cause failures, CCF, must be taken into account during the design of all SRP/CS conforming to categories 2 to 4.

For categories 3 and 4, the measures applied aim to avoid a failure simultaneously affecting the two functional channels.

For category 2, these measures aim to avoid a failure affecting both the functional and the test channels.

The measures to apply, recommended in Annex F of standard EN ISO 13849-1 can be used directly. When an SRP/CS is made up of several parts (e.g. an input "I", a logic "L" and an output "O"), an overall score must be determined taking the measures applied to each of the parts into account.

Note: The score is not calculated in proportion to how far these requirements are applied. Thus, for each requirement, the maximum score that can be awarded is achieved if the requirement is met **in full for all the parts making up the SRP/CS**. Otherwise, the score achieved is null.

In the example illustrated in Table 1 (SRP/CS including an input, a logic and an output), we notice that:

- for requirement No. 3.1, the recommended steps are met for the three parts making up the SRP/CS (I, L and O). The score awarded for this requirement (15) is achieved,
- for requirement No. 3.2, the recommended steps are adequate only for two (I and L) of the three parts making up the SRP/CS. The score awarded for this requirement (5) is not achieved.

Table 1: Example of scoring for measures against CCF

No.	Scoring for measures against CCF (Annex F – Informative - of the standard)			
	Input ("I") – Logic ("L") – Output ("O") =>	I	L	O
3	**Design/application/experience**			
3.1	*Protection against over-voltage, over- pressure, over- current, etc.* ***– Score achieved***	15		
	Fuse for the electrical part	X		
	Fuse for the electrical part		X	
	Pressure relief valve for the hydraulic part			X
3.2	*Components used are well-tried* ***– Score not achieved***	0		
	Well-tried component involving a positive opening principle	X		
	Well-tried component (contactor chosen and installed in line with Table D3 EN13849-2)		X	
	Un-tried hydraulic component (not defined in Annex C - EN13849-2)			N

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.

Extract 1: Extract of Table F.1 of EN ISO 13849-1 (formerly Table F.2)

Applying Table F1 to the standard (see Extract 1), the measures to avoid CCF are satisfactory when an overall minimum score of 65 is reached for a given SRP/CS.

6.6 Application of the "block method"

The simplified approach described in the standard requires a block-oriented logical representation of the SRP/CS. This "block method" is described in Annex B of the standard.

This method makes it possible to calculate the $MTTF_d$ for each channel and the DC_{avg} using the formulae for the simplified method. To be able to apply the block method to an SRP/CS, the designer must produce a diagram of the planned final control scheme. All the components for which failure is potentially dangerous must be identified. Each of these components will make up a block. The block representation must clearly reveal the separation between the two functional channels (if there is redundancy) and the test channel (if necessary).

6.7 Diagnostic coverage (DC) of dangerous failures

Reminder: *diagnostic coverage (DC) (see § 3.1.26 of the standard),*

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

The DC is classed in four levels based on percentages listed in Table 6 of the standard. An estimation of DC is presented in Annex E of the standard for the different types of measures implemented to determine the DC.

In most cases, this estimation is perfectly adequate. However, there are situations in which the designer must use the information supplied by the manufacturer of the component implemented (e.g. when using safety logic units, or some input cards for programmable safety components which allow several usage modes). In these cases, a DC must be determined for each individual case.

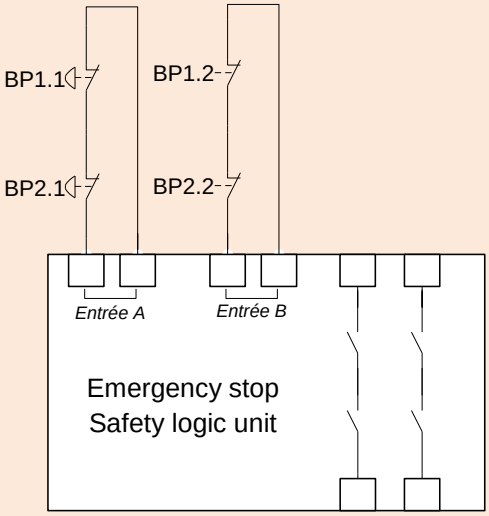
Warning 3

Serial input into a safety logic unit

When using a safety logic unit, it is important to adhere to the manufacturer's wiring recommendations and to take the specificities of the application into account, in particular when simultaneous commutation possibilities exist for input elements linked in series.

Example of how the DC changes with serial arrangement of push-button input to an emergency stop safety logic unit which can perform to PLe:

- when a single push-button can be activated at a time, the DC is generally greater than or equal to 99% (high DC),
- if several emergency stop buttons can be activated simultaneously, the DC is lower and it becomes impossible to achieve a PLe. Some manufacturers indicate a DC of 60% (low DC) when two emergency stops are connected.



When the manufacturer of the safety logic unit foresees the possibility of connecting several input elements in series, the corresponding DC value must be indicated as a function of the number of expected input components.

With more than two elements connected in series, it is recommended that the DC be considered to be below 60%, i.e. "null".

Example 8.2.34 in the BGIA Report 2/2008e[6] also notes that it is not possible to develop category 4 architecture when several inputs are connected in cascade on a single module.

In addition, the ISO/DIS 14119 draft standard[7] addresses this problem in its Annex J (*Evaluation of fault masking in serial connections of guard interlocking devices with potential-free contacts*) and provides a summary table stating the rule to be applied to determine the DC for cases where guard interlocking devices are connected in series on a safety module.

Number of frequently used movable guards[a]		Number of additional movable guards	Masking probability	DC for interlocking device limited to
1	+	1	low	low
		2 to 4	medium	low
		> 4	high	none
> 1			high	none
[a] If the frequency is higher than once per hour.				

Extract 2: Table J.1 from standard ISO/DIS 14119

[6] BGIA Report 2/2008e: Functional safety of machine controls – Application of EN ISO 13849
[7] ISO/DIS 14119: Safety of machinery - Interlocking devices associated with guards -- Principles for design and selection

6.8 Calculating $MTTF_d$ for pneumatic, mechanical and electromechanical components (Annex C of the standard)

For each channel in the designated architecture of an SRP/CS, the corresponding $MTTF_d$ value must be calculated based on the $MTTF_d$ values of the individual components implemented. For pneumatic, mechanical and electromechanical components, manufacturers supply a "B10d" characteristic which is necessary to calculate the $MTTF_d$ of these components. Indeed, as these elements contain parts which are subject to mechanical wear, the real usage conditions for the planned application must be considered. The method used to calculate the $MTTF_d$ of these components is summarised in Figure 7.

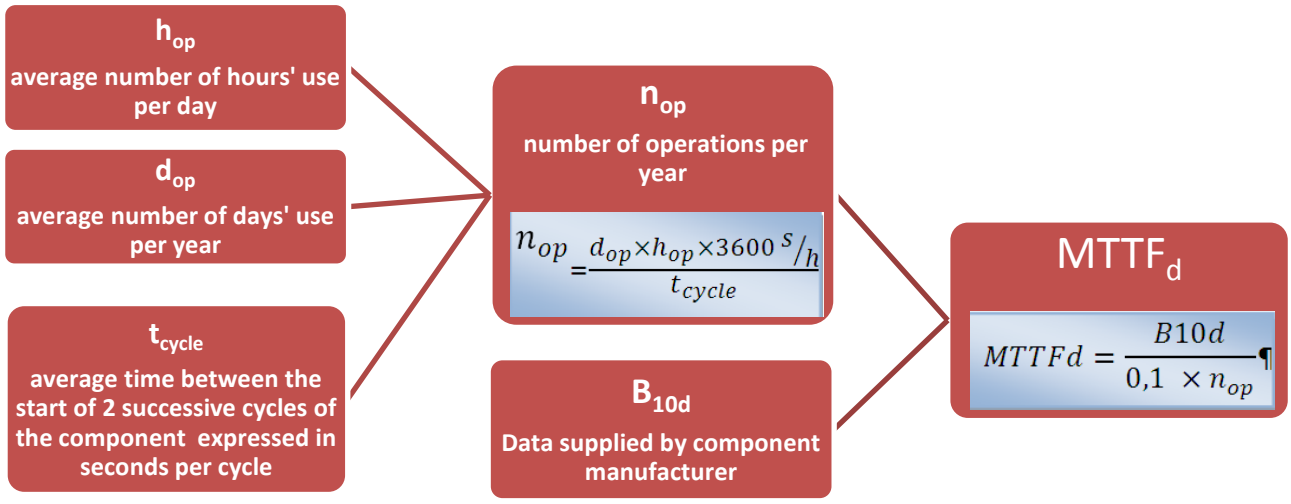


Figure 7: Calculating the $MTTF_d$ for a single component based on its B_{10d}

Note: t_{cycle} must use the real solicitation number for the component. This number may be greater than the solicitation of the safety function (e.g. when a component is shared between several functions with different levels of solicitation).

7 Combining several functions triggering the same actuator

When several safety functions, or one (or more) safety function(s) and one (or more) "standard" function(s) control stoppage of the same actuator, it is necessary to establish a relationship between these functions so that each one can play its independent role, or so that they act simultaneously, conserving, when necessary, the priority of safety functions over "standard" functions.

In practice, one or more parts of each safety or "standard" function will transmit stop orders from one or more safety functions to the actuator. An example is given in Figure 8.

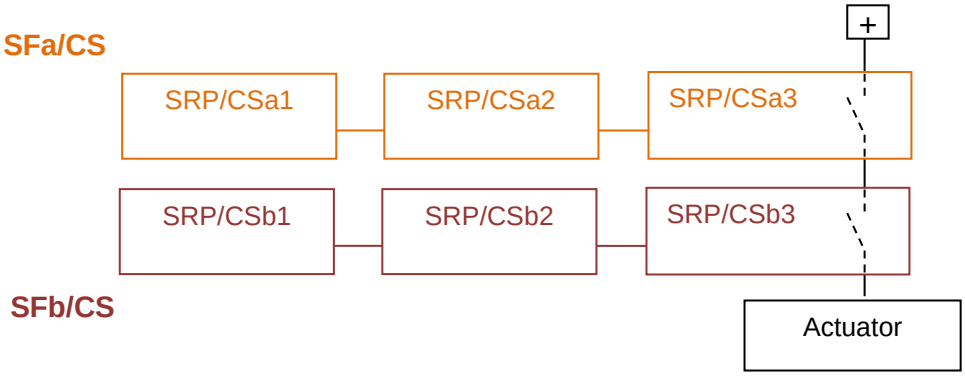


Figure 8: The signal from SFa/CS to the actuator passes through SRP/CSb3, which is an element of SFb/CS

In this example, the order to stop issued by safety function SFa passes through SRP/CSb3, which is an integral part of SFb/CS, before reaching the actuator. SRP/CSb3 does not play a functional role in safety function SFa.

Questions:

- Could safety function SFa be affected by failure of SRP/CSb3?
- If so, what effect would that have on the PL achieved by SFa/CS?

To answer these questions, the types of failure SRP/CSb3 may be subject to must be analysed to determine how these failures might affect the behaviour of safety function SFa.

Study of two sample set-ups:

1st case - SRP/CSb3 has potential-free contact outputs

In this case, failure of SRP/CSb3 has no effect on the behaviour of SFa/CS which remains fully operational.

The PL for SFa will be estimated taking only SRP/CSa1, SRP/CSa2 and SRP/CSa3 into account.

2nd case - SRP/CSb3 has electronic outputs

Figure 9 represents a case where potential-free contact outputs are used for function SFa and electronic outputs are used for SFb. Output for SFb (SRP/CSb3) is thought to have failed by reinjecting enough energy (represented by a red line) to supply the actuator.

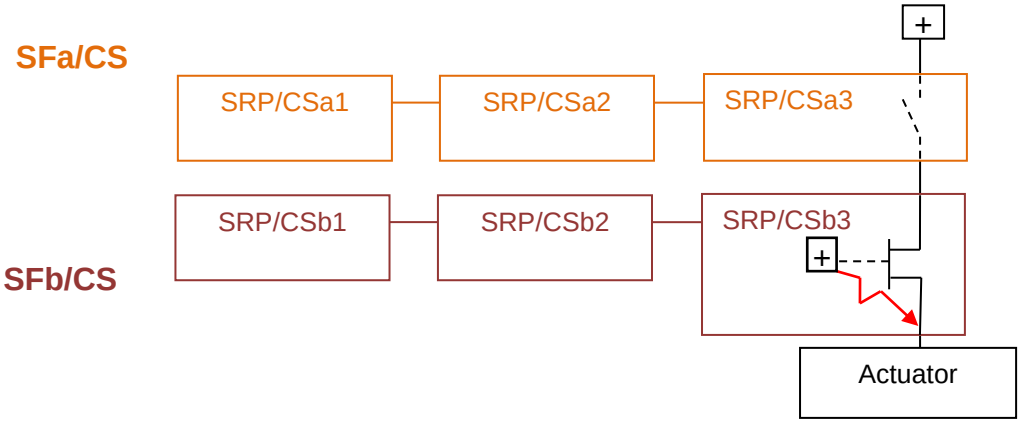


Figure 9: Example of failure of an electronic output

This failure is potentially dangerous to function SFb, since due to its failed output it can no longer order the actuator to stop. This failure is also potentially dangerous for function SFa. Opening the output contacts for this function no longer has any effect, and the actuator does not receive an order to stop.

The PL for SFa should therefore be calculated taking SRP/CSa1, SRP/CSa2, SRP/CSa3 and SRP/CSb3 into account.

Conclusions

When physical elements (elements of another safety function or another standard function) are inserted between a SF/CS and the actuator it controls (e.g. Figure 8), the influence of failure of these elements on the SF/CS in question must be analysed.

When failure of these elements has no effect on the SF/CS considered (e.g. potential-free contacts), they need not be taken into account when calculating the PL.

When failure of these elements affects the function of the SF/CS, it may be necessary to revise the design of the function(s) and/or to modify their placement in terms of the interconnections. If these elements are maintained, they must be taken into account when determining the PL of the SF/CS considered.

Warning: If failure of an element performing a "standard" function can affect a SF/CS, it should not be inserted between the SF/CS and its actuator.

8 Notes on the use of SISTEMA software

SISTEMA software assists designers in applying standard EN ISO 13849-1 by taking them through the different design phases recommended by the standard, and by calculating the necessary data without requiring external recourse to the mathematical formulae.

It offers the possibility of using reliability databases for components supplied by some manufacturers.

However, it does not explicitly deal with the steps to be implemented to take systematic failures into account. Thus, the designer must treat them separately by applying Annex G of the standard.

SISTEMA is not a substitute for extensive knowledge of the standard, since the design choices remain the prerogative of the designer. For example, it would be impossible to choose between a safety category and a designated architecture if the different characteristics were not known.

In addition, SISTEMA does not deal with the software elements of safety-related control systems.

Use of this software requires a learning period, since the terminology used is slightly different from that used in EN ISO 13849-1 (e.g. SRP/CS are called SB (for Subsystems) and the notion of elements (as a "sub unit" of a block), which does not appear explicitly in the standard, is introduced). Nevertheless, the breakdown into different elements suggested is very close to that of standard EN 62061.

Use of SISTEMA requires the same preparation as when the design is performed without using it, for example, the designer must:

- specify the safety function (SF),
- specify the SRP/CS (SB), the components (BL and/or EL),
- reflect on and choose the planned designated architecture,
- determine the reliability data for the components (B10d, $MTTF_d$) or choose to exclude failures - note that SISTEMA allows access to some libraries of "manufacturer's characteristics" or the default values for the standard,
- specify the measures against CCF - SISTEMA lists the steps from Annex F of the standard and offers a choice from among them or adoption of other measures,
- analyse potential failures to determine which parts should be considered,
- specify the diagnostic functions.

Finally, with or without SISTEMA, the control schemes for the functional and diagnostic parts must be designed adhering **strictly** to the specifications established and the design choices made.

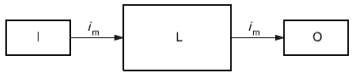
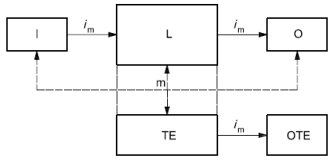
SISTEMA software facilitates repeated design and makes it possible to generate a final report. Like all software tools, SISTEMA provides traceability which makes it possible to treat projects as they evolve. It is therefore a useful tool provided it is used by personnel who are familiar with the standard, in complement to the standard, as a support and guide for the application of its recommendations.

Note: For the example SF/CS design dealt with in this document, the PL calculated by SISTEMA was the same as that obtained using the simplified method described in the standard.

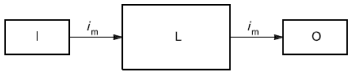
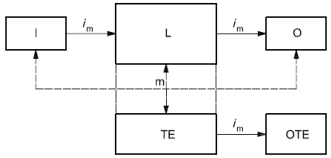
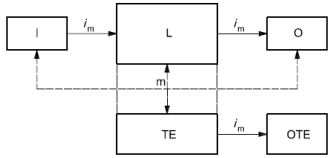
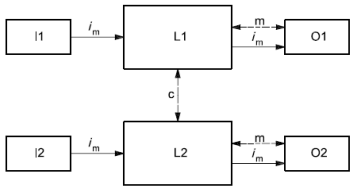
Annex 1: Tables of minimal recommendations to achieve a given PL

Minimal recommendations to achieve an "a" PL - Based on Table 7 and using the simplified procedure

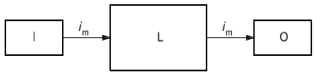
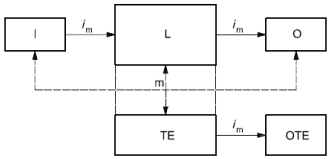
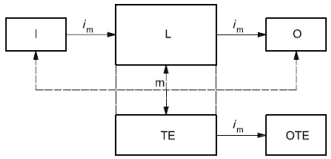
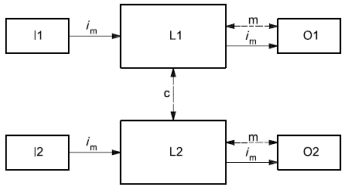
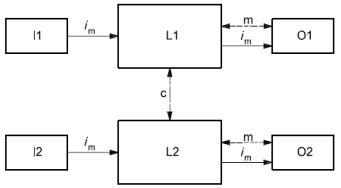
In the following tables, all citations (table, §, annexe) refer to standard EN ISO 13849-1

Authorised categories	**Cat B** *§ 6.2.3*	**Cat 2** *§ 6.2.5*
Respects another category		Respects the requirements of Cat B
$MTTF_d$ for each functional channel ***§ 4.5.2***	3 years ≤ $MTTF_d$ ≤ 100 years (i.e., $MTTF_d$ ≥ "Low")	3 years ≤ $MTTF_d$ ≤ 100 years (i.e., $MTTF_d$ ≥ "Low")
Minimum DC_{avg} ***§ 4.5.3 and Annex E***	DC_{avg} ≥ 0 (DC_{avg} ≥ "Null")	DC_{avg} ≥ 60% (i.e., DC_{avg} ≥ "Low")
CCF ***Annex F***	N.A.	Score ≥ 65
Specificities	Components appropriate for the function	- Well-tried components and safety principles (§ 6.2.4) - $MTTF_{d,TE}$ to be considered (§ 4.5.4)
check of Functions - periodicity	N.A.	Start of machine, and periodically (automatic or manual), and demand rate ≤ 1/100 test rate
check of Functions - reaction	N.A.	If fault detected: Put in a safe state (stopped) or warn of the danger
Designated architecture		
Systematic faults	Annex G	Annex G

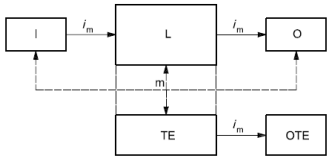
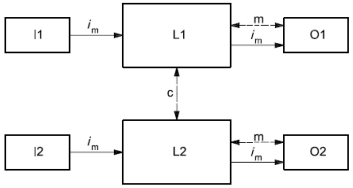
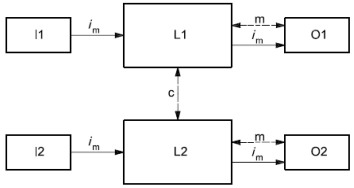
Minimal recommendations to achieve a "b" PL - Based on Table 7 and using the simplified procedure

Authorised categories	**Cat B** *§ 6.2.3*	**Cat 2** *§ 6.2.5*	**Cat 2** *§ 6.2.5*	**Cat 3** *§ 6.2.6*
Respects another category		Respects the requirements of Cat B	Respects the requirements of Cat B	Respects the requirements of Cat B
$MTTF_d$ for each functional channel ***§ 4.5.2***	10 years ≤ $MTTF_d$ ≤ 100 years (i.e., $MTTF_d$ ≥ "Medium")	10 years ≤ $MTTF_d$ ≤ 100 years (i.e., $MTTF_d$ ≥ "Medium")	3 years ≤ $MTTF_d$ ≤ 100 years (i.e., $MTTF_d$ ≥ "Low")	3 years ≤ $MTTF_d$ ≤ 100 years (i.e., $MTTF_d$ ≥ "Low")
Minimum DC_{avg} ***§ 4.5.3 and Annex E***	DC_{avg} ≥ 0 (DC_{avg} ≥ "Null")	DC_{avg} ≥ 60% (i.e., DC_{avg} ≥ "Low")	DC_{avg} ≥ 90% (i.e., DC_{avg} ≥ "Medium")	DC_{avg} ≥ 60% (i.e., DC_{avg} ≥ "Low")
CCF ***Annex F***	N.A.	Score ≥ 65	Score ≥ 65	Score ≥ 65
Specificities	Components appropriate for the function	- Well-tried components and safety principles (§ 6.2.4) - $MTTF_{d,TE}$ to be considered (§ 4.5.4)	- Well-tried components and safety principles (§ 6.2.4) - $MTTF_{d,TE}$ to be considered (§ 4.5.4)	- Well-tried component and safety principles (§ 6.2.4) - Single fault = safe state
check of Functions - periodicity	N.A.	Start of machine, and periodically (automatic or manual), and demand rate ≤ 1/100 test rate	Start of machine, and periodically (automatic or manual), and demand rate ≤ 1/100 test rate	If possible, at or before next solicitation
check of Functions - reaction	N.A.	If fault detected: Put in a safe state (stopped) or warn of the danger	If fault detected: Put in a safe state (stopped) or warn of the danger	If fault detected: Put in a safe state (stopped)
Designated architecture				
Systematic faults	Annex G	Annex G	Annex G	Annex G

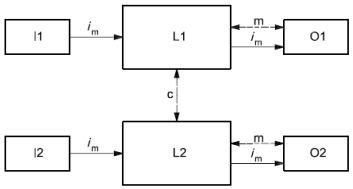
Minimal recommendations to achieve a "c" PL - Based on Table 7 and using the simplified procedure

Authorised categories	**Cat 1** *§ 6.2.4*	**Cat 2** *§ 6.2.5*	**Cat 2** *§ 6.2.5*	**Cat 3** *§ 6.2.6*	**Cat 3** *§ 6.2.6*
Respects another category	Respects the requirements of Cat B	Respects the requirements of Cat B	Respects the requirements of Cat B	Respects the requirements of Cat B	Respects the requirements of Cat B
$MTTF_d$ for each functional channel ***§ 4.5.2***	30 years ≤ $MTTF_d$ ≤ 100 years (i.e., $MTTF_d$ = "High")	30 years ≤ $MTTF_d$ ≤ 100 years (i.e., $MTTF_d$ = "High")	10 years ≤ $MTTF_d$ ≤ 100 years (i.e., $MTTF_d$ ≥ "Medium")	10 years ≤ $MTTF_d$ ≤ 100 years (i.e., $MTTF_d$ ≥ "Medium")	3 years ≤ $MTTF_d$ ≤ 100 years (i.e., $MTTF_d$ ≥ "Low")
Minimum DC_{avg} ***§ 4.5.3 and Annex E***	DC_{avg} ≥ 0 (DC_{avg} ≥ "Null")	DC_{avg} ≥ 60% (i.e., DC_{avg} ≥ "Low")	DC_{avg} ≥ 90% (i.e., DC_{avg} ≥ "Medium")	DC_{avg} ≥ 60% (i.e., DC_{avg} ≥ "Low")	DC_{avg} ≥ 90% (i.e., DC_{avg} ≥ "Medium")
CCF ***Annex F***	N.A.	Score ≥ 65	Score ≥ 65	Score ≥ 65	Score ≥ 65
Specificities	Well-tried component and safety principles	- Well-tried components and safety principles (§ 6.2.4) - $MTTF_{d,TE}$ to be considered (§ 4.5.4)	- Well-tried components and safety principles (§ 6.2.4) - $MTTF_{d,TE}$ to be considered (§ 4.5.4)	- Well-tried component and safety principles (§ 6.2.4) - Single fault = safe state	- Well-tried component and safety principles (§ 6.2.4) - Single fault = safe state
check of Functions - periodicity	N.A.	Start of machine, and periodically (automatic or manual), and demand rate ≤ 1/100 test rate	Start of machine, and periodically (automatic or manual), and demand rate ≤ 1/100 test rate	If possible, at or before next solicitation	If possible, at or before next solicitation
check of Functions - reaction	N.A.	If fault detected: Put in a safe state (stopped) or warn of the danger	If fault detected: Put in a safe state (stopped) or warn of the danger	If fault detected: Put in a safe state (stopped)	If fault detected: Put in a safe state (stopped)
Designated architecture					
Systematic faults	Annex G	Annex G	Annex G	Annex G	Annex G

Minimal recommendations to achieve a "d" PL - Based on Table 7 and using the simplified procedure

Authorised categories	**Cat 2** *§ 6.2.5*	**Cat 3** *§ 6.2.6*	**Cat 3** *§ 6.2.6*
Respects another category	Respects the requirements of Cat B	Respects the requirements of Cat B	Respects the requirements of Cat B
$MTTF_d$ for each functional channel ***§ 4.5.2***	30 years ≤ $MTTF_d$ ≤ 100 years (i.e., $MTTF_d$ = "High")	30 years ≤ $MTTF_d$ ≤ 100 years (i.e., $MTTF_d$ = "High")	10 years ≤ $MTTF_d$ ≤ 100 years (i.e., $MTTF_d$ ≥ "Medium")
Minimum DC_{avg} ***§ 4.5.3 and Annex E***	DC_{avg} ≥ 90% (i.e., DC_{avg} ≥ "Medium")	DC_{avg} ≥ 60% (i.e., DC_{avg} ≥ "Low")	DC_{avg} ≥ 90% (i.e., DC_{avg} ≥ "Medium")
CCF ***Annex F***	Score ≥ 65	Score ≥ 65	Score ≥ 65
Specificities	- Well-tried components and safety principles (§ 6.2.4) - $MTTF_{d,TE}$ to be considered (§ 4.5.4)	- Well-tried component and safety principles (§ 6.2.4) - Single fault = safe state	- Well-tried component and safety principles (§ 6.2.4) - Single fault = safe state
check of Functions - periodicity	Start of machine, and periodically (automatic or manual), and demand rate ≤ 1/100 test rate	If possible, at or before next solicitation	If possible, at or before next solicitation
check of Functions - reaction	If fault detected: Put in a safe state (stopped) or warn of the danger	If fault detected: Put in a safe state (stopped)	If fault detected: Put in a safe state (stopped)
Designated architecture			
Systematic faults	Annex G	Annex G	Annex G

Minimal recommendations to achieve an "e" PL - Based on Table 7 and using the simplified procedure

Authorised categories	**Cat 4** *§ 6.2.7*
Respects another category	Respects the requirements of Cat B
$MTTF_d$ for each functional channel ***§ 4.5.2***	30 years ≤ $MTTF_d$ ≤ 100 years (i.e., $MTTF_d$ = "High")
Minimum DC_{avg} ***§ 4.5.3 and Annex E***	DC_{avg} ≥ 99% (i.e., DC_{avg} = "High")
CCF ***Annex F***	Annex F (CCF ≥ 65)
Specificities	- Well-tried component and safety principles (§ 6.2.4) - Single fault = safe state
check of Functions - periodicity	at or before next solicitation
check of Functions - reaction	Fault detected: Put in a safe state (stopped)
Designated architecture	
Systematic faults	Annex G

Example of design of a SF/CS of PL_r "d" - Category 3

This example illustrates the design of a SF/CS composed of three SRP/CS, of which one has a known PL (central branch in Graph 1: General design process for a SF/CS conforming to a required PL)

All the design phases have been addressed and are recalled, highlighting the details. Comments deemed necessary to integrate the principles recommended by the standard and based on the graphs, tables and recommendations described in the previous part of this document are included.

The two SRP/CS of unknown PL were developed by applying paragraph 6 of this document. To facilitate comparisons with Graph 2: Details of the design of an SRP/CS to achieve a required PL , extracts of the graph are given at each design step.

The iterations necessary to treat the example are not listed in this document, which presents only the final version of the design phases.

A1. Presentation of the function

This SF/CS will ensure a safety function on a machine including a mobile working element. The rotational movement of this working element is controlled by a hydraulic motor. The risk is linked to the rotational movement (clockwise and anti-clockwise) of the tool. We chose to implement a movable guard to prevent acces to the mobile working element.

The safety function consists in stopping the rotational movement when the movable guard is open.

In this example, details are not given on how the required performance level (PL_r) was determined (see Annex A in the standard). The initial hypotheses are: **PL_r "d" and use of category "3" architecture**

A safety logic unit is chosen to ensure the logic part of the safety function.

To simplify the examples, the system activating the interlocking device for the movable guard and the hydraulic motor are not considered.

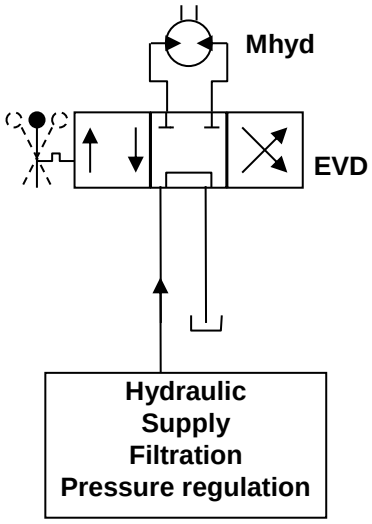


Figure 10: Basic hydraulic design

A2. Specifying the safety function

Specification of the functional requirements of the safety function	
No.	**Function name** Stop of hydraulic motor by the guard
Required performance level (based on risk estimation)	PL "d"
Conditions in which the function will be activated	This function is always active
SF/CS interface	Input: - Actuator of the interlocking device on the guard (e.g. activation cam). Output: - The 2 control orifices of the hydraulic motor.
Description of the function	This function consists in stopping and preventing rotational movement of the tool if the guard is open; if the guard is closed, rotational movement is authorised through the machine's control logic.
Priority relative to other simultaneous functions	This safety function must have priority over rotational movement (clockwise and anti-clockwise) ordered by the machine's control logic (EVD).
Other SF/CS acting on the same actuator	N.A.
Maximum reaction time for the SF/CS	The maximum reaction time between the input information and the output must not exceed 80 ms.
Demand rate of the function	The frequency of opening the guard is estimated to be 10 times per hour over an 8-hour period for 220 days/year.
Reaction to faults/Restart conditions	The reaction in case of a fault must stop and hold to stop the rotational movement of the tool. Restart can be authorised once the fault has been eliminated.
Environmental conditions	Minimal degree of protection given the foreseeable environment: PI 65

Table 2: Specification of the functional requirements of the safety function

A3. Basic logical structure

Based on the specification of the functional requirements for the function "Stop of hydraulic motor by the guard" (Table 2), the designer develops a logical structure (presented in Figure 11), based on his/her experience in designing similar machines and knowledge of components commonly used in this field. This task can be performed without pre-selecting the material to be used, but often the designer's experience gives them an idea of the type of material he/she expects to use. For example, in the case of this stop function, it is common to use at least one commercially available safety logic unit to facilitate the design and implementation phase.

For this function, the designer plans:

- An "input" part which will be composed of a interlocking device made up of position switch(es).
- A "logic" part, which will be composed of a "safety logic unit ". This type of component will make it possible to create the interface between the input interlocking device and the hydraulic output part. As there are a wide range of safety logic units available on the market, it is often advantageous to choose this option to avoid the need to develop an SRP/CS. This type of component will facilitate the designer's task when developing diagnostics and/or when redundancies.
- An "output" part, which must use hydraulics so as to interface with the hydraulic motor, will be composed of electrically-controlled hydraulic valve(s) so as to be compatible with the control logic of the machine. This part will be used to ensure that the SF/CS has priority over the standard control logic of the motor including EVD.
  By physically inserting this part between the standard part and the hydraulic motor, it is certain that the SF/CS will always perform its function, whatever the orders emitted by, or the failures of, the standard part (EVD).

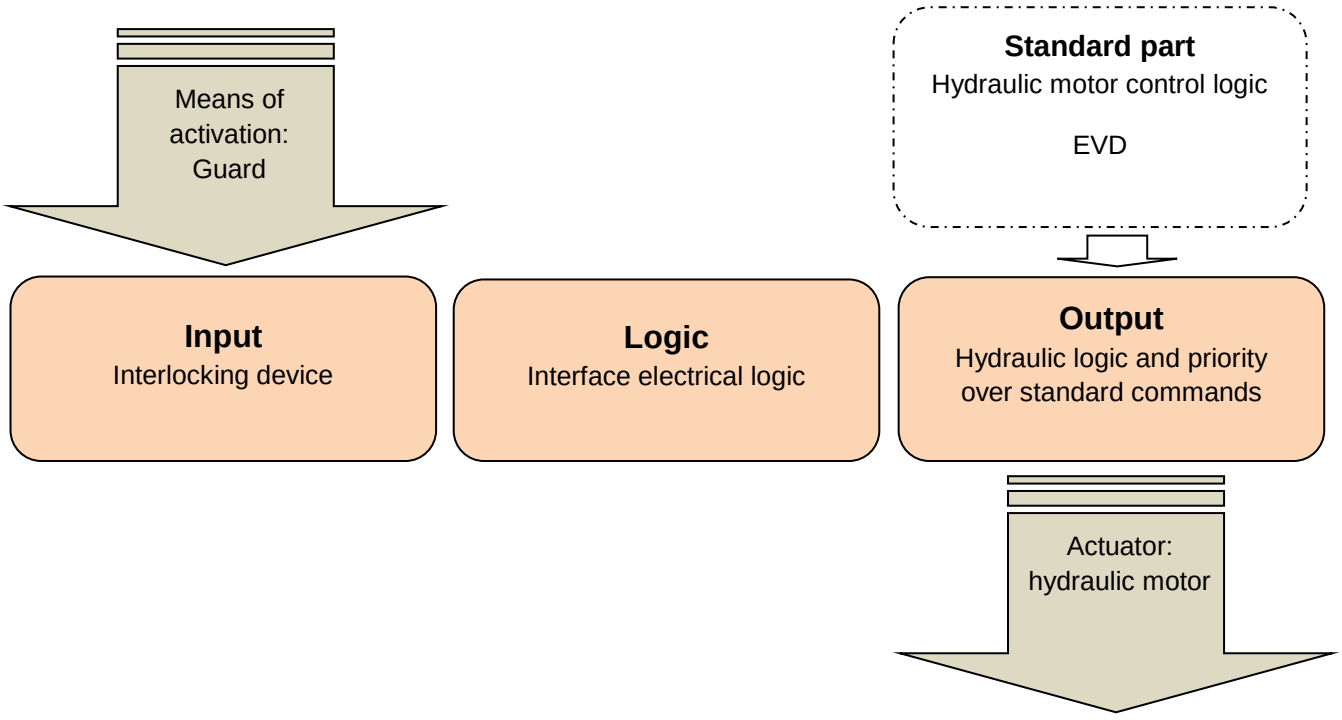


Figure 11: Basic logical structure for the SC/FS

A4. Definition of the necessary SRP/CS to create the SF/CS "Stop of hydraulic motor by the guard"

Given the logical structure planned for the SF/CS in § A3, the designer applies the central branch of Graph 1: General design process for a SF/CS conforming to a required PL, which consists in creating the SF/CS by associating a logical part of known PL - here a commercially available safety logic unit for the "logic" part - with parts of his/her own design for the input and output. The designer will thus plan to work on the basis of an SRP/CS for each entity in the basic logical structure of the SF/CS.

The design choice for this SF/CS is represented in Figure 12

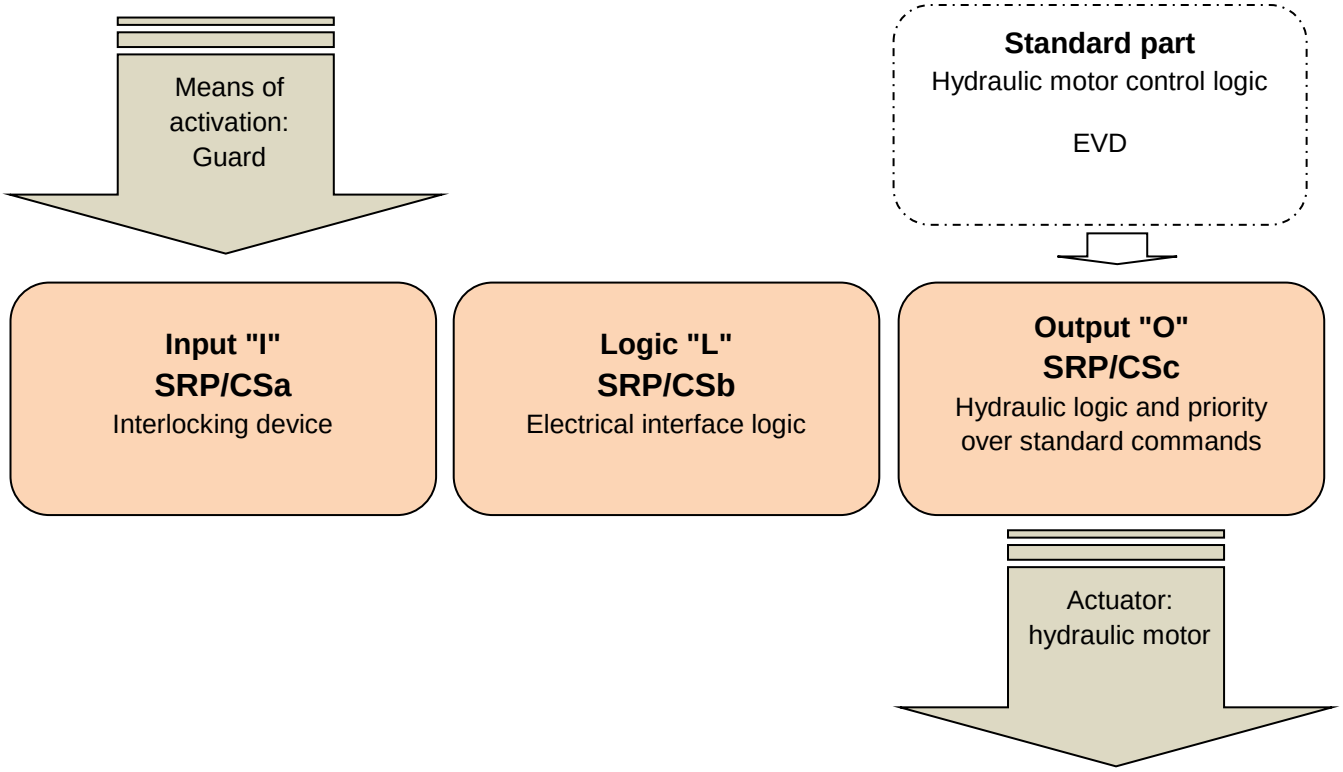
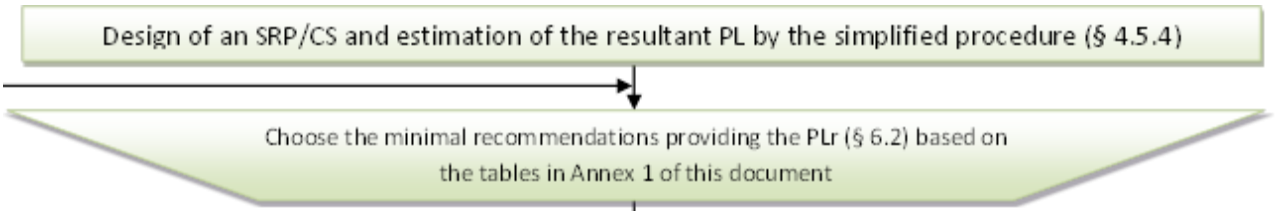


Figure 12: Design choice for the SC/FS

Note: As the SF/CS includes 3 SRP/CS, each SRP/CS must achieve a PL greater than or equal to the PLd required for the SF/CS (see Warning 2).

A5. Designing the SRP/CS

A5.1 Design of SRP/CSa



Extract of Graph 2: Details of the design of an SRP/CS to achieve a required PL

SRP/CSa must be designed to a PL of at least "d" respecting the corresponding criteria, summarised in Table 1 (extract of Annex 1 of this document). The designer chooses to start the process by selecting a category 3 architecture.

Minimal recommendations to achieve a "d" PL - Based [illegible] and using [illegible] simplified procedure

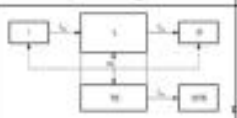
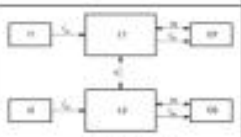
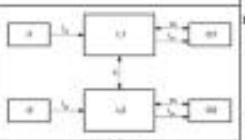
	Cat 2 § 6.2.5	Cat 3 § 6.2.6	Cat 3 § 6.2.6
Authorised categories			
Respects another category	Respects the requirements of Cat B	Respects the requirements of Cat B	Respects the requirements of Cat B
MTTFd for each functional channel § 4.5.2	30 years ≤ MTTFd ≤ 100 years (i.e., MTTFd = "High")	30 years ≤ MTTFd ≤ 100 years (i.e., MTTFd = "High")	10 years ≤ MTTFd ≤ 100 years (i.e., MTTFd ≥ "Medium")
Minimum DCavg § 4.5.3 and Annex E	DCavg ≥ 90% (i.e., DCavg ≥ "Medium")	DCavg ≥ 60% (i.e., DCavg ≥ "Low")	DCavg ≥ 90% (i.e., DCavg ≥ "Medium")
CCF Annex F	Score ≥ 65	Score ≥ 65	Score ≥ 65
Specificities	- Well-tried components and safety principles (§ 6.2.4) - MTTFd to be considered (§ 4.5.4)	- Well-tried component and safety principles (§ 6.2.4) - Single fault = safe state	- Well-tried component and safety principles (§ 6.2.4) - Single fault = safe state
check of Functions - periodicity	Start of machine, and periodically (automatic or manual), and demand rate ≤ 1/100 test rate	If possible, at or before next solicitation	If possible, at or before next solicitation
check of Functions - reaction	If fault detected Put in a safe state (stopped) or warn of the danger	If fault detected Put in a safe state (stopped)	If fault detected Put in a safe state (stopped)
Designated architecture			
Systematic faults	Annex G	Annex G	Annex G

Table 1: Minimal recommendations to achieve a PL "d"

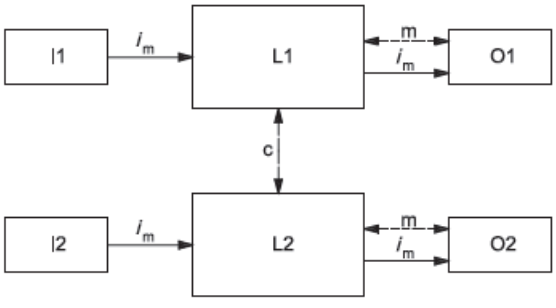
Example of design of a SF/CS of PL_r « d » - Category 3

The specifications of the SRP/CSa are deduced from those of the SF/CS (Table 2).

Specification of the Input SRP/CS	
	Name: SRP/CSa
Activation conditions	Always active
Interface	Input: - Actuator of the interlocking device on the guard (e.g. activation cam). Output: - 2 electrical signals, each representing the state of the guard - closed or not closed - transmitted to the terminals of the interlocking device.
Means of interconnection (i_{ab})	Between SPR/CSa and SPR/CSb: electrical cables exposed to the environmental constraints outside the electrical cabinet.
Description	As category 3 is targeted, this SRP/CS is designed in two channels. Each channel generates a logical state "0" as output when the guard is not closed, and a logical state "1" when the guard is closed.
Priorities	N.A.
Maximum reaction time	The sum of the times for the SPR/CS must not exceed the maximum reaction time specified for the SF/CS (80 ms).
Demand rate	The frequency of opening the guard is estimated to be 10 times per hour over an 8-hour period for 220 days/year.
Environmental conditions	Minimal degree of protection PI 65

Table 4: Specification of SRP/CSa

The architecture selected as the basis for the design is that shown in Figure 11 of the standard (see Extract 3)



Dashed lines represent reasonably practicable fault detection.

Key

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

Extract 3: Figure 11 from standard EN ISO 13849-1

Example of design of a SF/CS of PL_r « d » - Category 3

Implementation of the selected architecture.

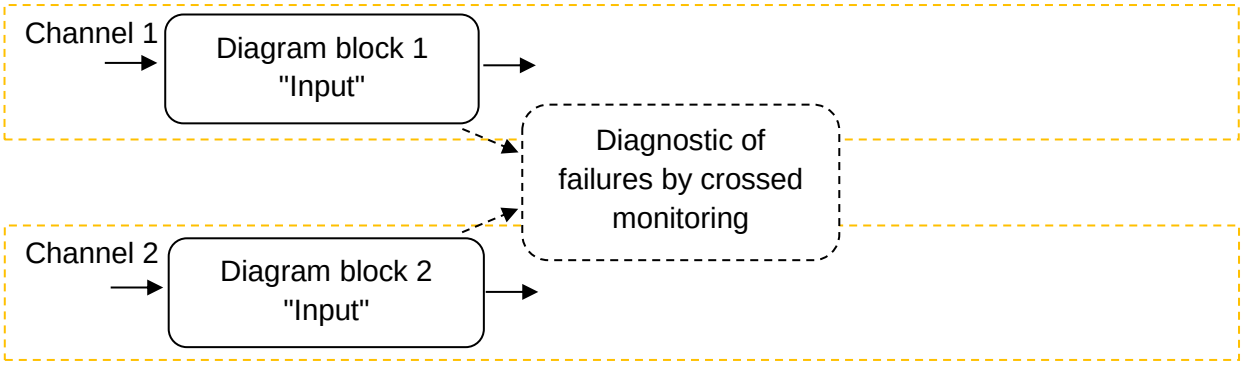
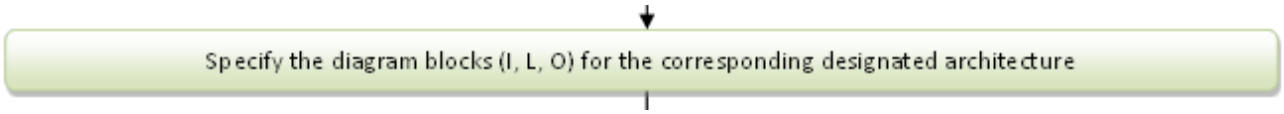
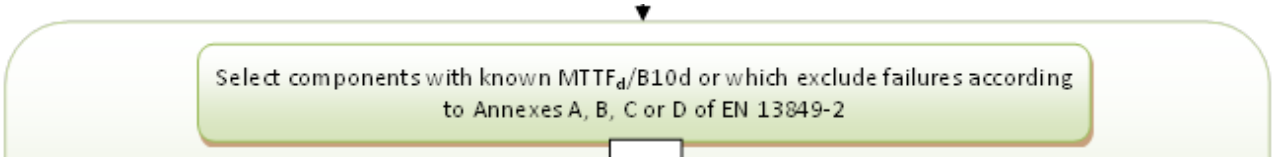


Figure 13: Breakdown of SRP/CSa with block diagrams



Extract from Graph 2: Details of the design of an SRP/CS to achieve a required PL

Each individual block ensures the entire function for each of the channels described in the specification for SRP/CSa. There is therefore no need to re-specify each block individually, the elements from the specification of SRP/CSa can be copied.



Extract from Graph 2: Details of the design of an SRP/CS to achieve a required PL

Choice of material for block diagram 1

The following choice is made (see Figure 14):

Electromechanical position roller switch "S1" with 1 "O"-type contact with direct opening action (in conformity with EN60947-5-1).

Switch will be triggered in the positive mode and installed in line with the manufacturer's recommendations.

For the selected component, the response time is null.

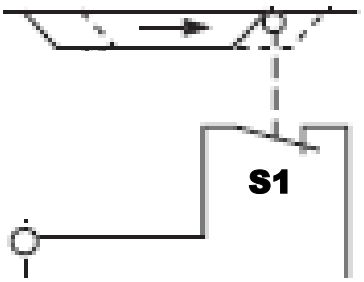


Figure 14: Switch S1 (shown in the closed guard configuration)

Choice of material for block diagram 2

The following choice is made (see Figure 15):

Electromechanical position roller switch "S2" with 1 "F"-type contact.

Switch will be installed in line with the manufacturer's recommendations.

For the selected component, the response time is null.

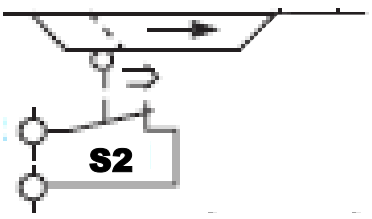
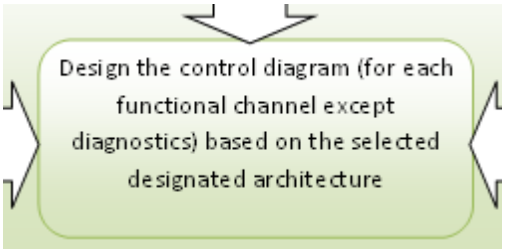


Figure 15: Switch S2 (shown in the closed guard configuration)

Example of design of a SF/CS of PL_r « d » - Category 3

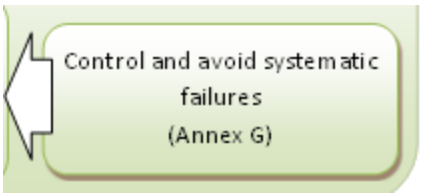
Design of the functional channel according to the category 3 designated architecture selected for the SRP/CS



Extract from Graph 2: Details of the design of an SRP/CS to achieve a required PL

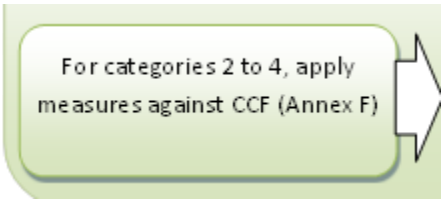
Channels 1 and 2 are composed of "**S1**" and "**S2**", respectively.

Systematic failures (see Annex A of this document)



Extract from Graph 2: Details of the design of an SRP/CS to achieve a required PL

Measures against CCF and scoring (see Table 5)



Extract from Graph 2: Details of the design of an SRP/CS to achieve a required PL

Table 5:Scoring of the measures against CCF for SRP/CSa

No.	Scoring of measures against CCF (Annex F – Informative - of the standard)	
1	**Separation/Segregation**	
	Physical separation between signal paths **– Score achieved**	***15***
	Separation by use of a different cable for each position switch	***x***
2	**Diversity**	
	Different design/technology or physical principles are used **– Score achieved**	***20***
	Different activation principle for the switches	***x***
3	**Design/application/experience**	
3.1	Protection against over-voltage, over-pressure, over-current, etc. **– Score achieved**	***15***
	Input fault taken into account by the safety logic unit	***x***
3.2	Components used are well-tried **– Score not achieved**	***0***
	No well-tried components are used	**N**

Example of design of a SF/CS of PL_r « d » - Category 3

4	**Assessment / analysis**	
	Are the results of a failure mode and effect analysis taken into account against common-cause-failures in design **– Score achieved**	***5***
	For the switches: common mechanical cause inexistent (principles of activation different due to inverted cam) - separate components	***x***
5	**Competence/training**	
	Score achieved	***5***
6	**Environmental**	
6.1	Prevention of contamination and electromagnetic compatibility (EMC) against CCF in accordance with appropriate standards**– Score achieved**	***25***
	Electromechanical parts not subject to EMC	***x***
6.2	Other influences **– Score achieved**	***10***
	Environmental requirements taken into account when selecting the switches (vibrations, humidity, temperature, shock) depending on the application constraints	***x***
	Total score	***95***
The total score is ≥ 65: The implemented measures meet the requirements		

Analysis of failure modes for each channel and their consequences

Extract from Graph 2: Details of the design of an SRP/CS to achieve a required PL

Component	**Type of fault retained**	**Consequence**	**Conclusion on the resultant potential danger (for the SRP/CS)** dangerous movement: D non-dangerous movement: ND
Switch **S1**	Welding of type "O" contact	Contact does not open	D
	Breaking of type "O" contact	Contact open	ND
	Activation system blocked "activated"	Contact open	ND
	Activation system blocked "de-activated" or broken	Contact does not open	D
Switch **S2**	Welding of type "F" contact	Contact does not open	D
	Breaking of type "F" contact	Contact open	ND
	Activation system blocked "activated"	Contact does not open	D
	Activation system blocked "de-activated" or broken	Contact open	ND

Table 6: Analysis of failure modes for components of SRP/CSa

Example of design of a SF/CS of PL_r « d » - Category 3

Specification of diagnostics and determination of DC

- Specify the diagnostic functions (role, frequency, reaction, etc.) for each component to be tested – *Annex E presents examples of useful diagnostic mechanisms.*
- Determine the DC for each component (§ 4.5.3 and Annex E).

Extract from Graph 2: Details of the design of an SRP/CS to achieve a required PL

Component and reminder of potentially dangerous faults	**Diagnostics planned** (based on Annex E of the standard)	**DC for each component** (according to Annex E of the standard)
Switch "**S1**" or "**S2**" Fault considered: Contact does not open	***Input*** *- Crossed monitoring of input without dynamic test*	99% (see note)
Note: Value retained given that all potentially dangerous faults are detected and that the frequency of diagnostic is judged to be high (tests performed systematically every time the guard is opened, i.e., 10 times per hour over an 8-h day, 220 days/year)		

Table 2: Diagnostic measures and estimation of DC

Component	**Specification and test rate**
Switches "**S1**" and "**S2**"	Crossed monitoring of the 2 switches is systematically performed every time the guard is opened, by the SRP/CSb (Safety logic unit).

Table 3: Specification of the diagnostic function of SRP/CSa

If a B10d is supplied, calculate the $MTTF_d$ for each component (using Annex C- §C4)

Extract from Graph 2: Details of the design of an SRP/CS to achieve a required PL

Determination of the $MTTF_d$ for individual components

Calculation of the $MTTF_d$ for each component is done using the formula in Figure 7, page 16

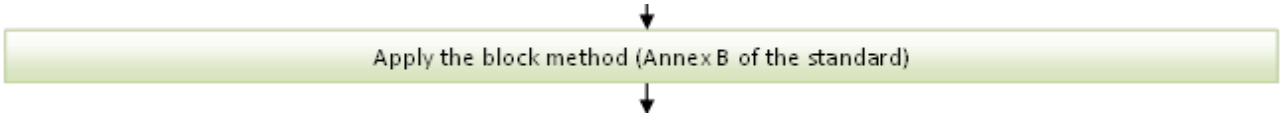
Reminder: The frequency of guard opening is estimated at 10 times per hour over an 8-h day, 220 days/year - demand frequency = 10 times per hour (3 600 s), thus t_{cycle} = 3 600/10 = 360 s

Component	**h_{op} (h)**	**d_{op}**	**n_{op} calculated**	**t_{cycle} (s)**	**B_{10d} manufacturer**	**Default B_{10d}** (Annex C in the standard)	**$MTTF_d$ calculated (years)**	**$MTTF_d$ manufacturer (years)**	**Default $MTTF_d$** (Annex C in the standard) **(years)**
S1	8	220	17600	360	50 000 000	/	28409		
S2	8	220	17600	360	50 000 000	/	28409		

Table 4: Determination of the $MTTF_d$ for each component in SRP/CSa

Example of design of a SF/CS of PL_r « d » - Category 3

Application of the "block method"



Extract from Graph 2: Details of the design of an SRP/CS to achieve a required PL

In the present case (Figure 16), each channel is made up of a single component

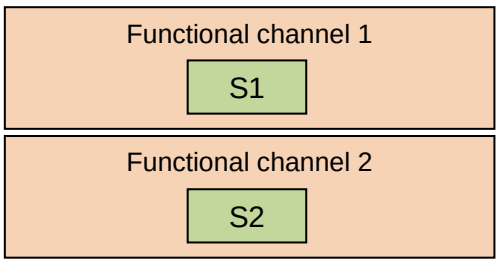
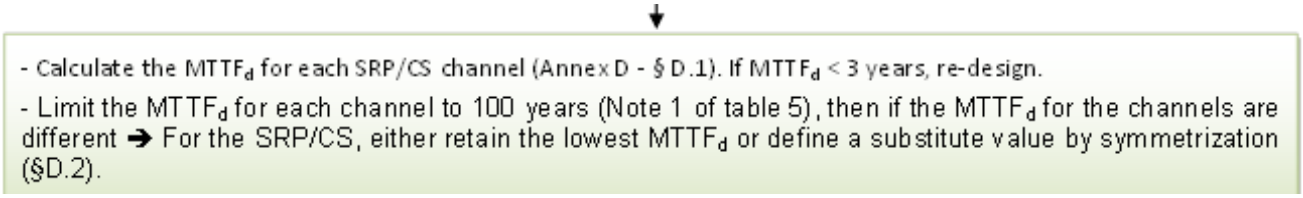


Figure 16: Diagram identifying the safety-related parts of SRP/CSa

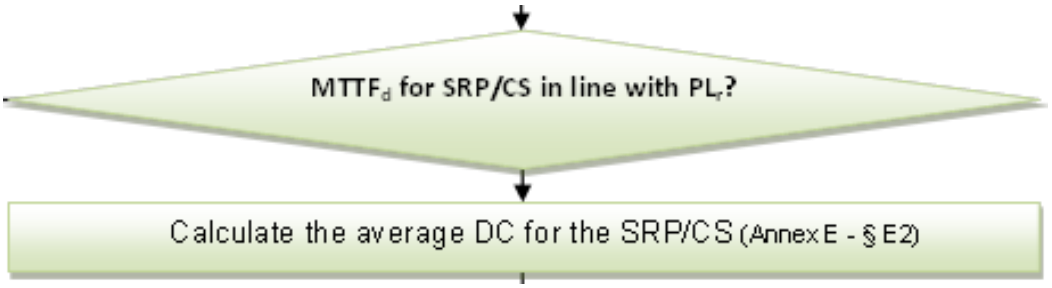


Extract from Graph 2: Details of the design of an SRP/CS to achieve a required PL

For each channel: the calculation gives $MTTF_d$ = 28409 years, limited to 100 years (Note 1 to Table 5 in the standard).

For SRP/CSa, as the two channels are symmetrical, **the $MTTF_d$ for each channel is equal to 100 years**.

$MTTF_d$ high meeting the requirements for PLd.

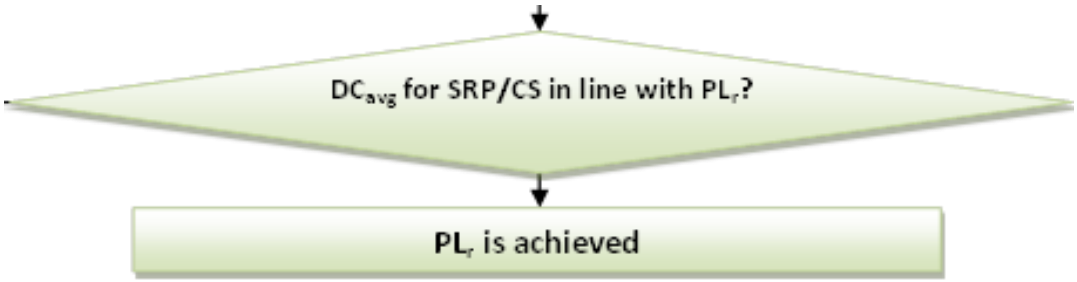


Extract from Graph 2: Details of the design of an SRP/CS to achieve a required PL

Example of design of a SF/CS of PL_r « d » - Category 3

The DC for S1 and S2 are 99%, the $MTTF_d$ for S1 and S2 are 100 years, thus the calculation gives:

$$DC_{avg} = \frac{\frac{DCS1}{MTTFdS1} + \frac{DCS2}{MTTFdS2}}{\frac{1}{MTTFdS1} + \frac{1}{MTTFdS2}} = 99\%$$ **i.e., DC_{avg} high meeting the requirements for PLd.**



Extract from Graph 2: Details of the design of an SRP/CS to achieve a required PL

Example of design of a SF/CS of PL_r « d » - Category 3

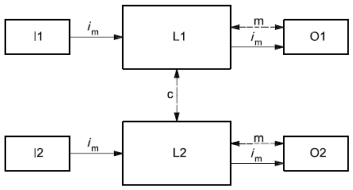
<table>
<tr><th colspan="4">Summary table for SRP/CSa</th></tr>
<tr><th>Data</th><th colspan="2">Requirements</th><th>Results obtained</th></tr>
<tr><td rowspan="8">Requirements for a PLd using category 3 architecture</td><td colspan="2">Respects requirements for Cat B</td><td>OK</td></tr>
<tr><td>30 years ≤ $MTTF_d$ ≤ 100 years
(i.e., $MTTF_d$ = "High")</td><td>10 years ≤ $MTTF_d$ ≤ 100 years
(i.e., $MTTF_d$ ≥ "medium")</td><td>$MTTF_d$ channel = 100 years
$MTTF_d$ High</td></tr>
<tr><td>DC_{avg} ≥ 60%
(i.e., DC_{avg} ≥ "Low")</td><td>DC_{avg} ≥ 90%
(i.e., DC_{avg} ≥"Medium")</td><td>DC_{avg} = 99%
DC_{avg} High</td></tr>
<tr><td colspan="2">CCF: score ≥ 65</td><td>Score = 95</td></tr>
<tr><td colspan="2">Well-tried component and safety principles
Single fault = safe state</td><td>OK
OK</td></tr>
<tr><td colspan="2">Tests: if possible, at or before next solicitation</td><td>Tests: at each solicitation</td></tr>
<tr><td colspan="2">If fault detected: put in a safe state (stopped)</td><td>If fault detected:
Safe state = stopped</td></tr>
<tr><td colspan="2"> 
</td><td>Category 3</td></tr>
<tr><td>Taking systematic faults into account</td><td colspan="2">Annex G</td><td>OK</td></tr>
<tr><td>Software</td><td colspan="2">§ 4.6 and Annex J</td><td>Not applicable</td></tr>
<tr><td colspan="3">Conclusion: PL "d" achieved?</td><td>YES</td></tr>
</table>

Table 5: Summary of the results obtained for SRP/CSa

Note: Based on the results obtained, SRP/CSa meets the minimal requirements to be awarded a PL "e". This call for a higher PL than necessary to meet the PL_r of the SF/CS can be useful when combining SRP/CS (see Table 11 in the standard).

Example of design of a SF/CS of PL_r « d » - Category 3

A5.2 Design of SRP/CSb

For SRP/CSb, a safety logic unit capable of achieving a PL "e" will be implemented, as this is the perfomance level most commonly available for this type of component (logic unit with a PL "d" are rare). The study will integrate this module to ensure that the PL "e" is achieved for this SRP/CS.

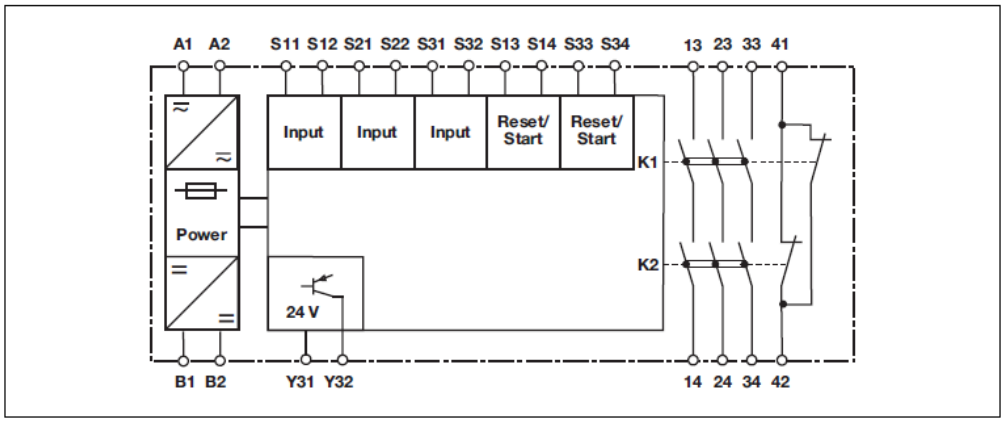
Specification of the Processing SRP/CS	
	Name: SRP/CSb
Activation conditions	Always active
Interface	Input: - 2 electrical signals emitted by SRP/CSa Output: - 2 electrical signals
Means of interconnection (i_{ab},i_{bc})	Between SPR/CSa and SPR/CSb: dealt with in SPR/CSa. Between SPR/CSb and SPR/CSc: dealt with in SPR/CSc.
Description	This part treats the redundancy of the interlocking device. Each output signal is in a "0" logical state when one of the two inputs is in a "0" logical state and in a "1" logical state when both inputs are in state "1".
Priorities	Not applicable
Maximal reaction time	The sum of the reaction times for the SPR/CS must not exceed the maximum reaction time specified for the SF/CS (80 ms).
Demand rate	The logic unit commutes each time the guard is solicited. The frequency of commutation of the logic unit is estimated at 10 times per hour over an 8-h day, 220 days/year.
Environmental conditions	Minimal degree of protection IP 65

Table 6: Specification for SRP/CSb

The choice was made to use a commercially available logic unit with a performance level "up to PLe", the description of how it works meets the functional specifications set out in Table 6.

So that SRP/CSb, and thus the logic unit, effectively achieves a PLe, the manufacturers requirements (not translated in English) , shown in Figure 17 and Figure 18, were respected.

Block diagram



Up to PL e of EN ISO 13849-1

Function description

- Single-channel operation: no redundancy in the input circuit, earth faults in the reset and input circuit are detected.
- Dual-channel operation with detection of shorts across contacts: redundant input circuit, detects
  - earth faults in the reset and input circuit,
  - short circuits in the input circuit and, with a monitored reset, in the reset circuit too,
  - shorts between contacts in the input circuit.
- Automatic start: Unit is active once the input circuit has been closed.
- Monitored reset: Unit is active once the input circuit is closed and once the reset circuit is closed after the waiting period has elapsed (see technical details).
- Increase in the number of available instantaneous safety contacts by connecting contact expansion modules or external contactors.

Key

- Power: Supply voltage
- Reset/Start: Reset circuit S13-S14, S33-S34
- Input: Input circuits S11-S12, S21-S22, S31-S32
- Output safe: Safety contacts 13-14, 23-24, 33-34
- Output aux: Auxiliary contacts 41-42
- Out semi CH: Semiconductor output switch status channel 1/2
- ①: Automatic reset
- ②: Monitored reset
- t_1: Switch-on delay
- t_2: Delay-on de-energisation
- t_3: Recovery time
- t_4: Waiting period

Wiring

Please note:

- Information given in the "Technical details" must be followed.
- Outputs 13-14, 23-24, 33-34 are safety contacts, output 41-42 is an auxiliary contact (e.g. for display).
- To prevent contact welding, a fuse should be connected before the output contacts (see technical details).
- Calculation of the max. cable runs I_{max} in the input circuit:

$$I_{max} = \frac{R_{lmax}}{R_l / km}$$

R_{lmax} = max. overall cable resistance (see technical details)
R_l /km = cable resistance/km

- Use copper wire that can withstand 60/75 °C.
- Sufficient fuse protection must be provided on all output contacts with capacitive and inductive loads.

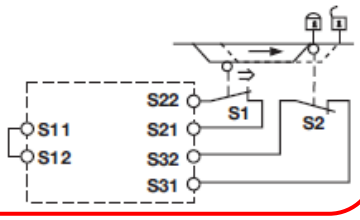
Déf systématiques

Figure 17: Extract from the manufacturer's instructions for the safety logic unit

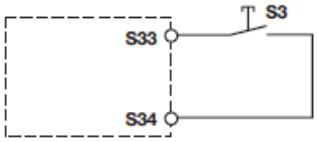
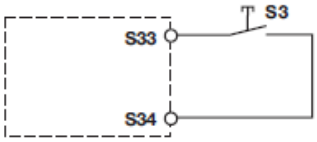
Example of design of a SF/CS of PL_r « d » - Category 3

The recommended connection diagram, taking potential short-circuits at input into account (requirement of behaviour when a fault is found at the level of SRP/CSa), retained to achieve a PLe is as follows:

- Input circuit

Input circuit	Single-channel	Dual-channel
Safety gate **with** detection of shorts across contacts Type of connection retained for input in the manufacturer's instructions		

- Reset circuit

Reset circuit	E-STOP wiring (single-channel) Safety gate (single-channel)	E-STOP wiring (dual-channel) Safety gate (dual-channel)
Automatic reset	Type of connection retained for reset in the manufacturer's instructions	
Monitored reset		

- Feedback loop

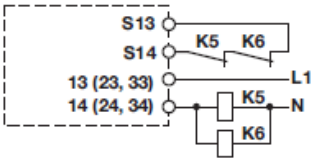
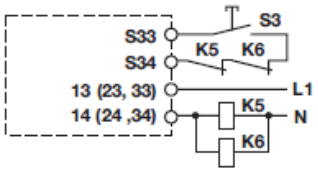
Feedback loop	Automatic reset	Monitored reset
Contacts from external contactors		

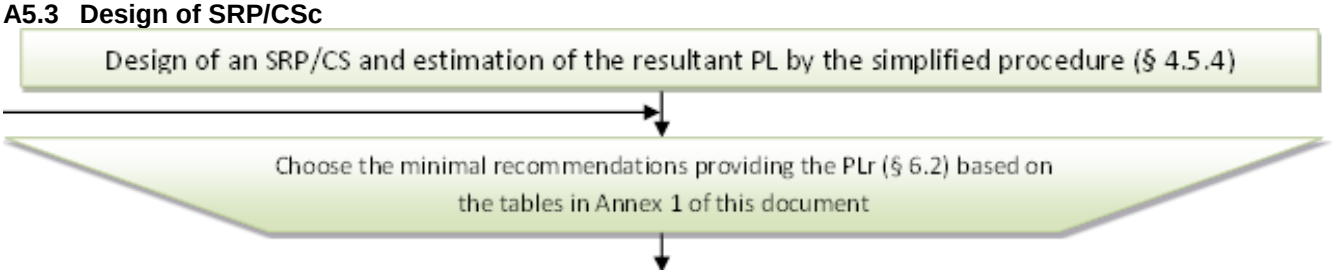
Figure 18: Extract from the manufacturer's instructions for the safety logic unit

Systematic failures (See Annex A of this document)

Prevention and control of systematic failures is achieved by following the instructions for use of the safety module, in particular by:

- installing correctly calibrated fuses on the power circuit for the output contacts,
- not exceeding the admissible load on the output contacts (cut-off capacity),
- respecting the length and type of cables transmitting input signals to the logic unit,
- placing the logic unit in an electrical cabinet with IP > 65.

A5.3 Design of SRP/CSc



Extract from Graph 2: Details of the design of an SRP/CS to achieve a required PL

SRP/CSc must be designed to achieve a PL of at least "d" by respecting the corresponding criteria, summarised in Table 7 extracted from Annex 1 of this document. Category 3 architecture is retained.

Minimal recommendations to achieve a "d" PL - Based on Table 7 and using the simplified procedure

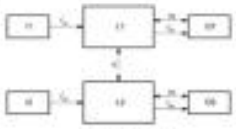
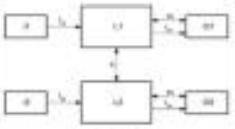
Authorised categories	Cat 2 § 6.2.5	Cat 3 § 6.2.6	Cat 3 § 6.2.6
Respects another category	Respects the requirements of Cat B	Respects the requirements of Cat B	Respects the requirements of Cat B
MTTFd for each functional channel § 4.5.2	30 years ≤ MTTFd ≤ 100 years (i.e., MTTFd = "High")	30 years ≤ MTTFd ≤ 100 years (i.e., MTTFd = "High")	10 years ≤ MTTFd ≤ 100 years (i.e., MTTFd ≥ "Medium")
Minimum DCavg § 4.5.3 and Annex E	DCavg ≥ 90% (i.e., DCavg ≥ "Medium")	DCavg ≥ 60% (i.e., DCavg ≥ "Low")	DCavg ≥ 90% (i.e., DCavg ≥ "Medium")
CCF Annex F	Score ≥ 65	Score ≥ 65	Score ≥ 65
Specificities	- Well-tried components and safety principles (§ 6.2.4) - MTTFd to be considered (§ 4.5.4)	- Well-tried component and safety principles (§ 6.2.4) - Single fault = safe state	- Well-tried component and safety principles (§ 6.2.4) - Single fault = safe state
check of Functions - periodicity	Start of machine, and periodically (automatic or manual), and demand rate ≤ 1/100 test rate	If possible, at or before next solicitation	If possible, at or before next solicitation
check of Functions - reaction	If fault detected Put in a safe state (stopped) or warn of the danger	If fault detected Put in a safe state (stopped)	If fault detected Put in a safe state (stopped)
Designated architecture			
Systematic faults	Annex G	Annex G	Annex G

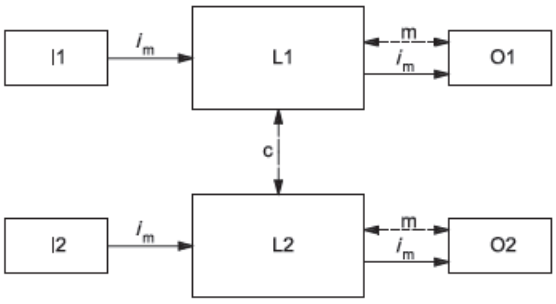
Table 7: Minimal recommendations to achieve a PL "d"

Example of design of a SF/CS of PL_r « d » - Category 3

Spécification of the Output SRP/CS	
	Name: SRP/CSc
Activation conditions	Always active
Interface	Input: - 2 electrical signals from output of SRP/CSb Output: - command orifices of the hydraulic motor.
Means of interconnection (i_{bc})	Between SRP/CSb and SRP/CSc: electrical cables subjected to the environmental constraints outside the electrical cabinet.
Description	This part stops and prevents supply of hydraulic fluid to the motor if one of the inputs is in a "0" logical state, and authorises supply of hydraulic fluid to the motor if both inputs are in a "1" state.
Priorities	Higher Priority over the standard hydraulic commands.
Maximum reaction time	The sum of the reaction times for the SPR/CS must not exceed the maximum reaction time specified for the SF/CS (80 ms).
Demand rate	The components implemented commute each time the guard is solicited. The frequency of commutation of the components is estimated at 10 times per hour over an 8-h day, 220 days/year.
Environmental conditions	Minimal degree of protection IP 65

Table 8: Specification of SRP/CSc

The architecture retained as the basis for the design is set by the standard (cf. figure 11), see Extract 1.



Dashed lines represent reasonably practicable fault detection.

Key

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

Extract 1: Figure 11 from standard EN ISO 13849-1

Example of design of a SF/CS of PL_r « d » - Category 3

Implementation of the architecture retained.

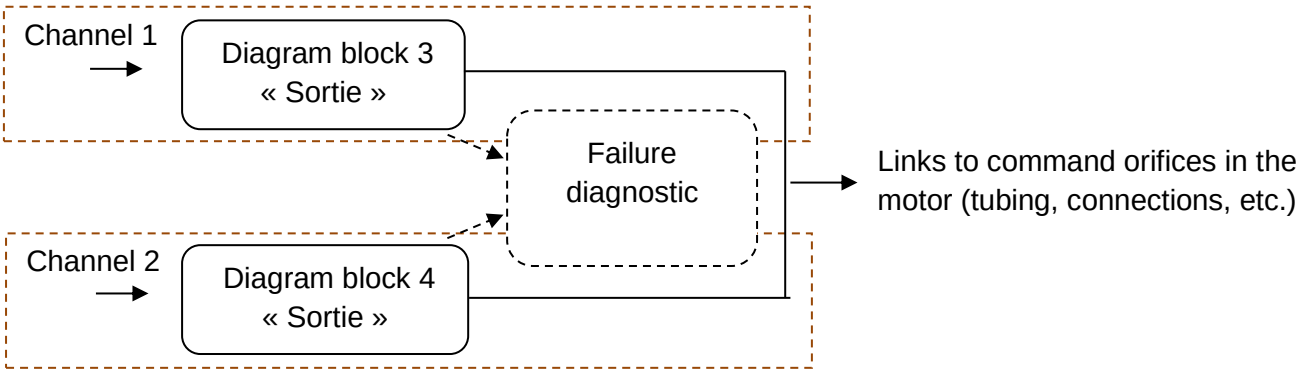
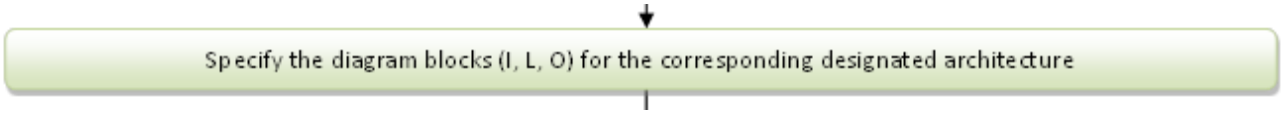
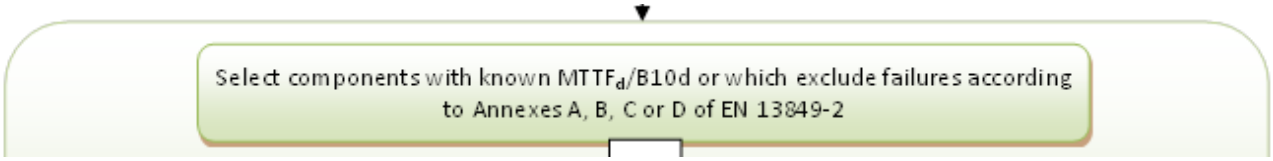


Figure 19: Breakdown of SRP/CSc with diagram block



Extract from Graph 2: Details of the design of an SRP/CS to achieve a required PL

Each block ensures the whole of the function of each of the channels described in the specification for SRP/CSc. Thus, there is no need to re-specify each block, it is sufficient to recall the elements of the specification of SRP/CSc.



Extract from Graph 2: Details of the design of an SRP/CS to achieve a required PL

Choice of material identical for block diagrams 3 and 4

The following choice is made (see Figure 20):

Two 4/2 (4 orifices/2 positions) hydraulic valves.

When their coils are supplied with electricity, they transfer the hydraulic power from EVD to the motor.

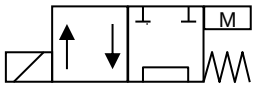


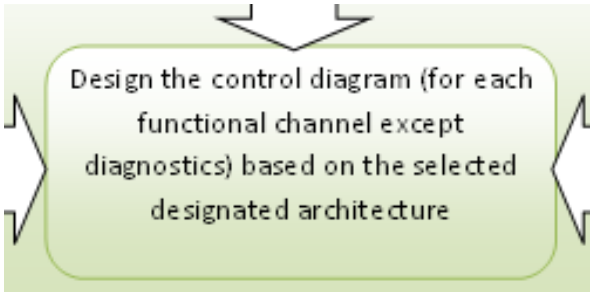
Figure 20: 4/2 hydraulic valve

When their coils are no longer supplied with electricity, they stop the rotational movement of the motor whatever the position of the directional command valve EVD of the hydraulic motor and they transfer the hydraulic power to the reservoir.

For the components selected, the response time is 30 ms.

Example of design of a SF/CS of PL_r « d » - Category 3

Design of the functional channel according to the category 3 designated architecture retained for the SRP/CS



Extract from Graph 2: Details of the design of an SRP/CS to achieve a required PL

Channels 1 and 2 are composed of "**SV1**" and "**SV2**", respectively.

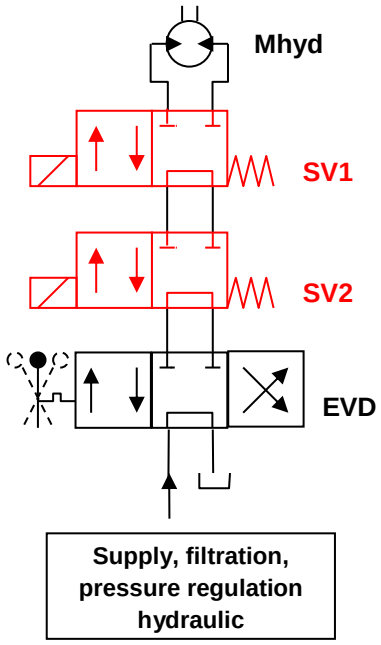
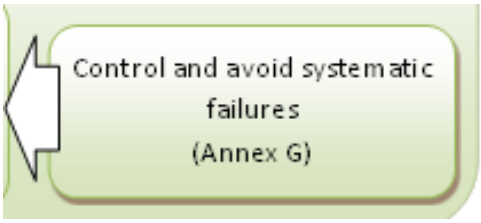


Figure 21: Diagram of the hydraulics to be implemented

Systematic failures (See Annex A of this document)

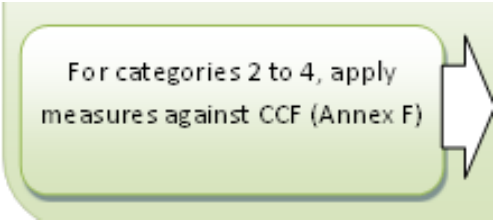


Extract from Graph 2: Details of the design of an SRP/CS to achieve a required PL

The elements taken into account must also include the means to link up to the command orifices of the motor (tubing, connections, etc.).

Example of design of a SF/CS of PL_r « d » - Category 3

Measures against CCF and scoring (see Table 9)



Extract from Graph 2: Details of the design of an SRP/CS to achieve a required PL

Table 9: Scoring of measures against CCF for SRP/CSc

No.	Scoring of measures against CCF (Annex F – Informative - of the standard)	
1	**Separation/Segregation**	
	Physical separation between signal paths **– Score achieved**	***15***
	Separation by use of a separate power cable for each of the hydraulic valves	***x***
2	**Diversity**	
	Different technologies/design or physical principles are used **– Score not achieved**	***0***
	/	**N**
3	**Design/application/experience**	
3.1	Protection against over-voltage, over-pressure, over-current, etc. **– Score achieved**	***15***
	Electrical protection (over-current) ensured at the level of supply to the outputs of the module (SRP/CSb) *Hydraulic protection (over-pressure) ensured at the level of hydraulic supply*	***x***
3.2	Components used are well-tried **– Score achieved**	***5***
	Use of hydraulic components designed according to well-tried safety principles	***x***
4	**Assessment/analysis**	
	Are the results of a failure mode and effect analysis taken into account to avoid common-cause-failures in design **– Score achieved**	***5***
	The main potential CCF for hydraulic distributors is linked to the quality of the hydraulic fluid. This is taken into account by preventing contamination of the hydraulic fluid (see 6.1)	***x***
5	**Competence/training**	
	Score achieved	***5***
6	**Environmental**	
6.1	Prevention of contamination and electromagnetic compatibility (EMC) against CCF in accordance with appropriate standards. **– Score achieved**	***25***
	Electromechanical command of hydraulic valves not subject to EMC *Hydraulic supply filtered at the level of the pressurised medium*	***x***
6.2	Other influences **– Score achieved**	***10***
	Environmental requirements taken into account when choosing the hydraulic valves (vibrations, humidity, temperature, shock) according to the constraints of the application.	***x***
	Total score	***80***
The total score is ≥ 65: The implemented measures meet the requirements		

Example of design of a SF/CS of PL_r « d » - Category 3

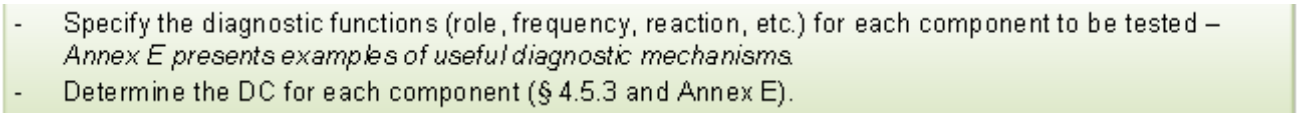
Analysis of failure modes for each of the channels and their consequences:

Extract from Graph 2: Details of the design of an SRP/CS to achieve a required PL

Component	**Type of failure retained**	**Consequence**	**Conclusion on the potential resultant danger (for the SRP/CS)** Dangerous movement: **D** Non-dangerous movement: **ND**
Hydraulic valve **SV1**	Mechanical blockage, broken spring	Valve remains activated	D
	Mechanical blockage or ruptured coil	Valve at rest	ND
Hydraulic valve **SV2**	Mechanical blockage, broken spring	Valve remains activated	D
	Mechanical blockage or ruptured coil	Valve at rest	ND

Table 10: Analysis of the failure modes for components of SRP/CSc

Specification of diagnostic procedures and determination of DC:



Extract from Graph 2: Details of the design of an SRP/CS to achieve a required PL

Component **and reminder of the potentially dangerous faults**	**Diagnosis planned** (based on Annex E of the standard)	**DC for each component** (according to Annex E of the standard)
Hydraulic valve **SV1** or **SV2** Fault considered: Valve remains activated	***Output device*** *- Direct monitoring of the electrical position of the control valves*	99%

Table 11: Diagnostic measures and estimation of the DC

Component	**Specification and test rate**
Hydraulic valve **SV1** or **SV2**	The electrical position of the control valves is directly monitored every time the hydraulic valves are solicited, and thus every time the guard is opened, by SRP/CSb (module).

Table 12: Specification of the diagnostic function of SRP/CSc

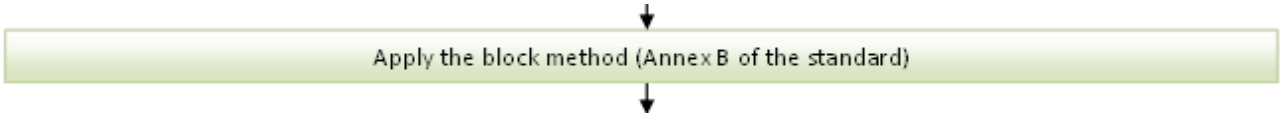
Example of design of a SF/CS of PL_r « d » - Category 3

Extract from Graph 2: Details of the design of an SRP/CS to achieve a required PL

Determination of the $MTTF_d$ for individual components

In the present case, in the absence of manufacturer's data, the $MTTF_d$ for each component is determined using the typical values from Table C.1 in the standard, i.e., 150 years for SV1 and SV2.

Application of the "block method"



Extract from Graph 2: Details of the design of an SRP/CS to achieve a required PL

In the present case (Figure 22), each channel is composed of a single component

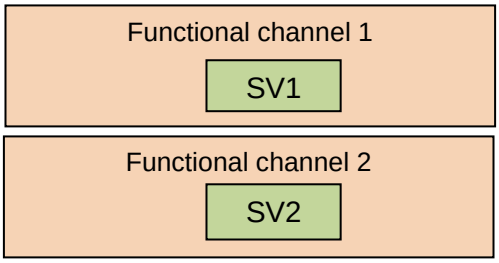
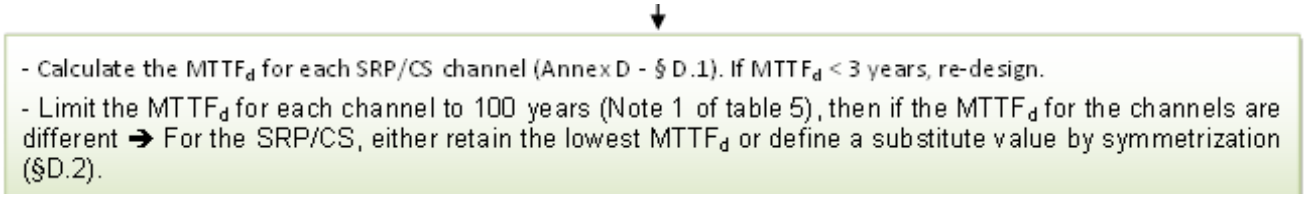
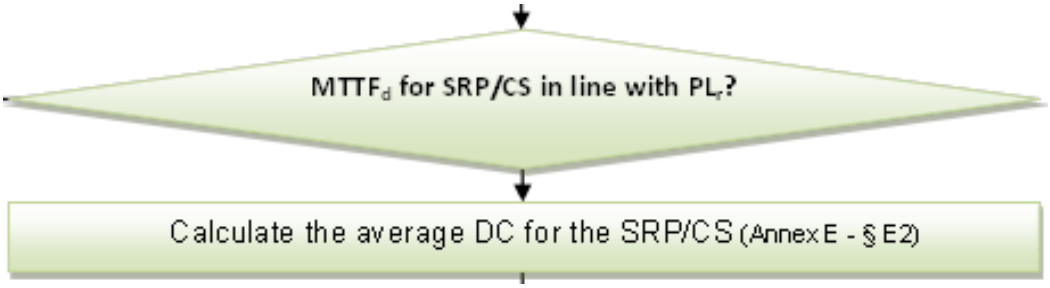


Figure 22: Diagram identifying the safety-related parts of SRP/CSc



Extract from Graph 2: Details of the design of an SRP/CS to achieve a required PL

For each channel: $MTTF_d$ = 150 years, limited to 100 years (Note 1 to Table 5 of the standard)
For SRP/CSc, as the two channels are symmetrical, the **$MTTF_d$ for each channel is equal to 100 years**.
$MTTF_d$ high meeting the requirements for PLd.

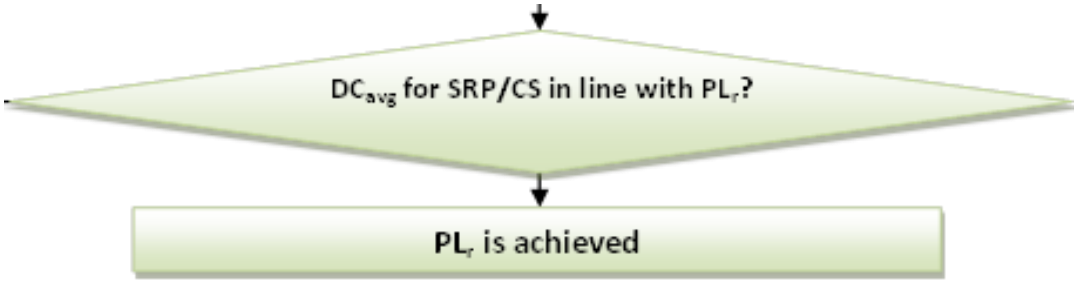


Extract from Graph 2: Details of the design of an SRP/CS to achieve a required PL

Example of design of a SF/CS of PL_r « d » - Category 3

The DC for SV1 and SV2 are 99%, the $MTTF_d$ for SV1 and SV2 are 100 years, the calculation is as follows:

$$DC_{avg} = \frac{\frac{DCEVS1}{MTTFdEVS1} + \frac{DCEVS2}{MTTFdEVS2}}{\frac{1}{MTTFdEVS1} + \frac{1}{MTTFdEVS2}}$$ **= 99% i.e., DC_{avg} high meeting the requirements for PLd.**



Extract from Graph 2: Details of the design of an SRP/CS to achieve a required PL

Example of design of a SF/CS of PL_r « d » - Category 3

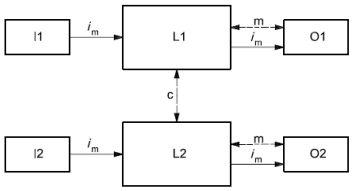
<table>
<tr><th colspan="4">Summary table for SRP/CSc</th></tr>
<tr><th>Data</th><th colspan="2">Requirements</th><th>Results obtained</th></tr>
<tr><td rowspan="8">Requirements to achieve a PLd when using category 3 architecture</td><td colspan="2">Respects requirements for Cat B</td><td>OK</td></tr>
<tr><td>30 years ≤ $MTTF_d$ ≤ 100 years
(i.e., $MTTF_d$ = "High")</td><td>10 years ≤ $MTTF_d$ ≤ 100 years
(i.e., $MTTF_d$ ≥ "Medium")</td><td>$MTTF_d$ channel = 100 years
$MTTF_d$ High</td></tr>
<tr><td>DC_{avg} ≥ 60%
(i.e., DC_{avg} ≥ "Low")</td><td>DC_{avg} ≥ 90%
(i.e., DC_{avg} ≥ "Medium")</td><td>DC_{avg} = 99%
DC_{avg} High</td></tr>
<tr><td colspan="2">CCF: score ≥ 65</td><td>Score = 80</td></tr>
<tr><td colspan="2">Well-tried component and safety principles
Single fault = safe state</td><td>OK
OK</td></tr>
<tr><td colspan="2">Tests: If possible, at or before next solicitation</td><td>Tests: at each solicitation</td></tr>
<tr><td colspan="2">If fault detected: Put in a safe state (stopped)</td><td>If fault detected:
Safe state = stopped</td></tr>
<tr><td colspan="2"> 
</td><td>Category 3</td></tr>
<tr><td>Systematic faults taken into account</td><td colspan="2">Annex G</td><td>OK</td></tr>
<tr><td>Software</td><td colspan="2">§ 4.6 and Annex J</td><td>Not applicable</td></tr>
<tr><td colspan="3">Conclusion: PL "d" achieved?</td><td>YES</td></tr>
</table>

Table 13: Summary of results obtained for SRP/CSc

Note: Given the results obtained, SRP/CSc satisfies the minimal requirements to be awarded a PL "e". This call for a higher PL than necessary to meet the PL_r of the SF/CS can be useful when combining SRP/CS (see Table 11 in the standard).

Example of design of a SF/CS of PL_r « d » - Category 3

A6. Final results for the SF/CS

A6.1 Determination of the PL for the SF/CS

The PL for each of the SRP/CS was determined in paragraphs A5.1, A5.2 and A5.3; the overall PL for the SF/CS is determined using Table 11 in the standard.

For the considered SF/CS, the combination of SRP/CS is represented in Figure 23

Figure 23: Combination of the SRP/CS to reach an overall PL

The **PL_{low}** for the three SRP/CS is PL **d**, which is applicable for 2 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.			

Figure 24: Use of Table 11 from standard EN ISO 13849-1

According to Table 11 of the standard, **the PL for the SF/CS is: PL d**

A6.2 Reaction time for the SF/CS

The reaction time is determined by taking the response time for the different SRP/CS making up the SF/CS into account.

Response time	SRP/Csa	SRP/CSb	SRP/CSc	SF/CS
	0	30 ms	30 ms	60 ms

Table 14: Reaction time for the SF/CS

The reaction time of 60 ms is acceptable as it is less than 80 ms, the maximum reaction time specified for the SF/CS in Table 2.

A6.3 Final diagram of the SF/CS

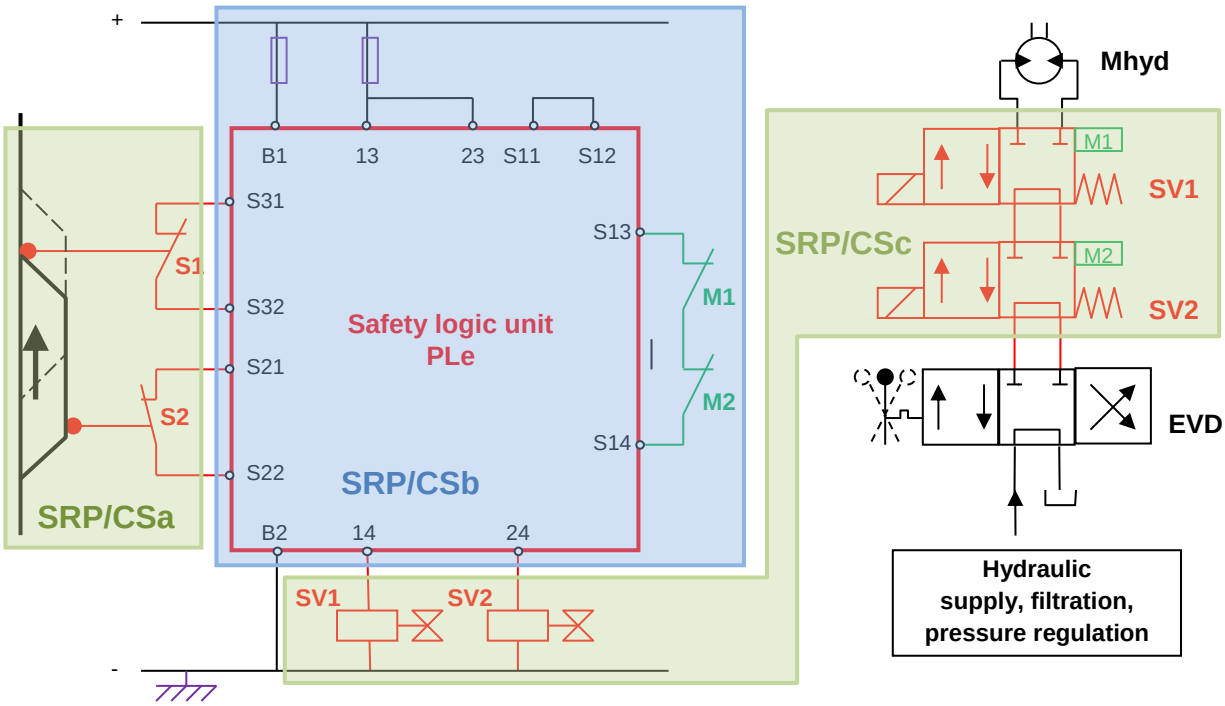


Figure 25: Final diagram of the SF/CS

Annex A - Systematic failures of all the SRP/CS in the SF/CS "Stop of hydraulic motor by the guard"

Table 20 describes the means implemented to cover systematic failures specific to this example of a SRP/CS. All the requirements from standard EN ISO 13849-1 are reported in the shaded areas. Some of the safety principles listed in ISO 13849-2 and references to tables in the annexes applicable to this example are also cited.

The measures implemented are indicated in green.

Systematic failures are taken into account as described hereafter, considering each SRP/CS ("a", "b", "c").

Table 20: Taking systematic failures into account

No.	***Systematic failures (Annex G - Informative - of the standard)***				
	SRP/CSa "a" – SRP/CSb "b" – SRP/CSc "c" =>		***a***	***b***	***c***
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*				
G2.1	- *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.*		***x***	***x***	***x***
	E.g. "Basic" electrical (see Table D.1 of ISO 13849-2) **and hydraulic** (see Table C.1 of ISO 13849-2) **safety principles**				
	Use of the de-energization principle	Opening the guard causes the contacts on position switches S1 and S2 to open, resulting in opening of the (F-type) contacts in the safety module. This de-energizes valves SV1 and SV2	***x***	***x***	***/***
		Hydraulic distributers SV1 and SV2 have a spring return. Their de-energization causes an interruption or fluid returns to baseline. A loss of power to the hydraulic system (loss of pressure) is not dangerous. A loss of pressure leads to a safe state (stops the dangerous movement)	***/***	***/***	***x***
G2.2	- *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).*		***x***	***x***	***x***
	E.g. "Basic" electrical (see Table D.1 of ISO 13849-2) **safety principles**				
	Use of the de-energization principle	Variations in power supply are controlled by the safety logic unit and lead to opening of the safety outputs if the limits are exceeded	***x***	***x***	***x***
	Protection against unforeseen restart	If the power supply comes back on, the guard must first be closed before the safety outputs can be closed. Thus there is no risk	***x***	***x***	***x***

G2.3	- *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).*			***x***	***x***	***x***
	E.g. "Basic" electrical (see Table D.1 of ISO 13849-2) **and hydraulic** (see Table C.1 of ISO 13849-2) **safety principles**					
	Resistance to environmental constraints	For electromagnetic interference and its effects	The electromechanical materials used are not sensitive to this radiation	***x***	***/***	***x***
			The safety logic unit itself meets these requirements and installation instructions are followed.	***/***	***x***	***/***
		For humidity, water and dust	IP 65 for the position switch and the hydraulic valve. Material designed for industrial use	***x***	***/***	***x***
			The safety module IP 40 is placed in an electrical cabinet conforming to IP 65	***/***	***x***	***/***
		Vibrations and shocks	Not applicable for this machine	***/***	***/***	***/***
G2.4	- *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).*			***/***	***/***	***/***
	N.A. none of the SRP/CS contains software			***/***	***/***	***/***
G2.5	*Measures for controlling the effects of errors and other effects arising from any data communication process (see IEC 61508-2:2000, 7.4.8)*			***/***	***/***	***/***
	N.A.: All the information relating to the SRP/CS are treated using hardwired logic.			***/***	***/***	***/***
	In addition, one or more of the following measures should be applied, taking into account the complexity of the SRP/CS and its PL:					
G2.6.1	- *failure detection by automatic tests*			***/***	***/***	***x***
	Detection of failures of the hydraulic valves **SV1** and **SV2** by monitoring **M1** and **M2**			***/***	***/***	***x***
G2.6.2	- *tests by redundant hardware*			***x***	***x***	***x***
	Verification of discordance between input S1 and S2 (SRP/CSa) using safety logic unit (SRP/CSb) Internal verification of the two safety logic unit pathways (SRP/CSb) Verification of the state of the hydraulic valves SV1 and SV2 (SRP/CSc) using safety logic unit (SRP/CSb)			***x***	***x***	***x***
G2.6.3	- *diverse hardware*			***/***	***/***	***/***
	Not implemented					
G2.6.4	- *operation in the positive mode*			***x***	***/***	***/***
	Switch **S1** activated in positive mode			***x***	***/***	***/***

G2.6.5	- *mechanically linked contacts*	/	/	/
	Not implemented			
G2.6.6	- *direct opening action*	x	/	/
	Contact for switch **S1** has direct opening action	x	/	/
G2.6.7	- *oriented mode of failure*	/	/	/
	Not implemented			
G2.6.8	- *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.*	/	/	/
	Not implemented			
G2.7	*(See ISO 13849-2:2003, D.3)*	x	x	x
G.3 Measures for avoidance of systematic failures *The following measures should be applied*				
G3.1	- *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.*	x	/	x
	Electromechanical (components and conductors) and hydraulic materials designed for industrial use and for the use planned in this application.	x	/	x
G3.2	- *Correct dimensioning and shaping* *Consideration of, e.g. stress, strain, fatigue, temperature, surface roughness, tolerances, manufacturing.*	x	/	/
	Characteristics of the switches activating the system should be adapted to the movements of the guard (working angle for the rollers of switches, alignment, etc.)	x	/	/
G3.3	- *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.*	x	x	x
	Respect of standard EN60204-1 *Conforms to the instructions for the safety* logic unit *Conforms to standard EN ISO 4413:2010 for the assembly of hydraulic components*	x	x	x
	E.g. "Basic" electrical (see Table D.1 of ISO 13849-2) **safety principles**			
	Adequate protection circuit: Each coil terminal of SV1 and SV2 valves solenoids and an electrical supply terminal of the safety relay are connected to the protection circuit.	/	x	x
	Isolation monitoring: A fuse is installed on the conductor which is not earthed so as to automatically break the circuit after an earthing fault.	/	x	x
	Isolation monitoring: The safety logic unit takes earthing faults at input into account.	x	/	/
	Protection against unexpected restart: In this application, re-establishing the command circuit is not dangerous as the guard must be closed to authorise restart and, thus, any risk is eliminated.	/	x	x

	Protection of the control circuit	The electrical control circuit is protected by appropriate and calibrated fuses.	***x***	***x***	***x***
	E.g. "Well-tried" electrical (see Table D.2 of ISO 13849-2) **safety principles**				
	Separation distance	Physical separation of the terminals on conductors which could present a risk if unforeseen connections could happen.	***x***	***x***	***x***
	E.g. "Basic" hydraulic (see Table C.1 of ISO 13849-2) **safety principles**				
	Pressure limitation	The hydraulic control circuit is protected against pressure surges by appropriate, calibrated means.	***/***	***/***	***x***
	Avoiding contamination of the fluid as far as possible	The hydraulic supply system is equipped with an appropriate filter which is checked regularly.	***/***	***/***	***x***
G3.4	- *Compatibility* *Use components with compatible operating characteristics*		***x***	***x***	***x***
	E.g. "Basic" electrical (see Table D.1 of ISO 13849-2) **safety principles / measures based on"state of the art" knowledge**				
	Compatibility	Electrical components compatible with the voltage and current used. Hydraulic component adapted to the pressures and flow-rates of the applications.	***x***	***x***	***x***
G3.5	- *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 13849-2:2002, D.2).*		***x***	***x***	***x***
	See G2.3		***x***	***x***	***x***
G3.6	- *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).*		***x***	***/***	***x***
	Electromechanical contacts and hydraulic valves with known failure modes		***x***	***/***	***x***
	In addition, one or more of the following measures should be applied, taking into account the complexity of the SRP/CS and its PL.				
G3.7.1	- *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).*		***X***	***X***	***X***
G3.7.2	- *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).*		***/***	***/***	***/***
G3.7.3	- *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).*		***/***	***/***	***/***
	Given the low complexity of this application, analyses were performed without design or simulation tools		***/***	***/***	***/***

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.*				
	*** not treated in this document**	*****	*****	*****