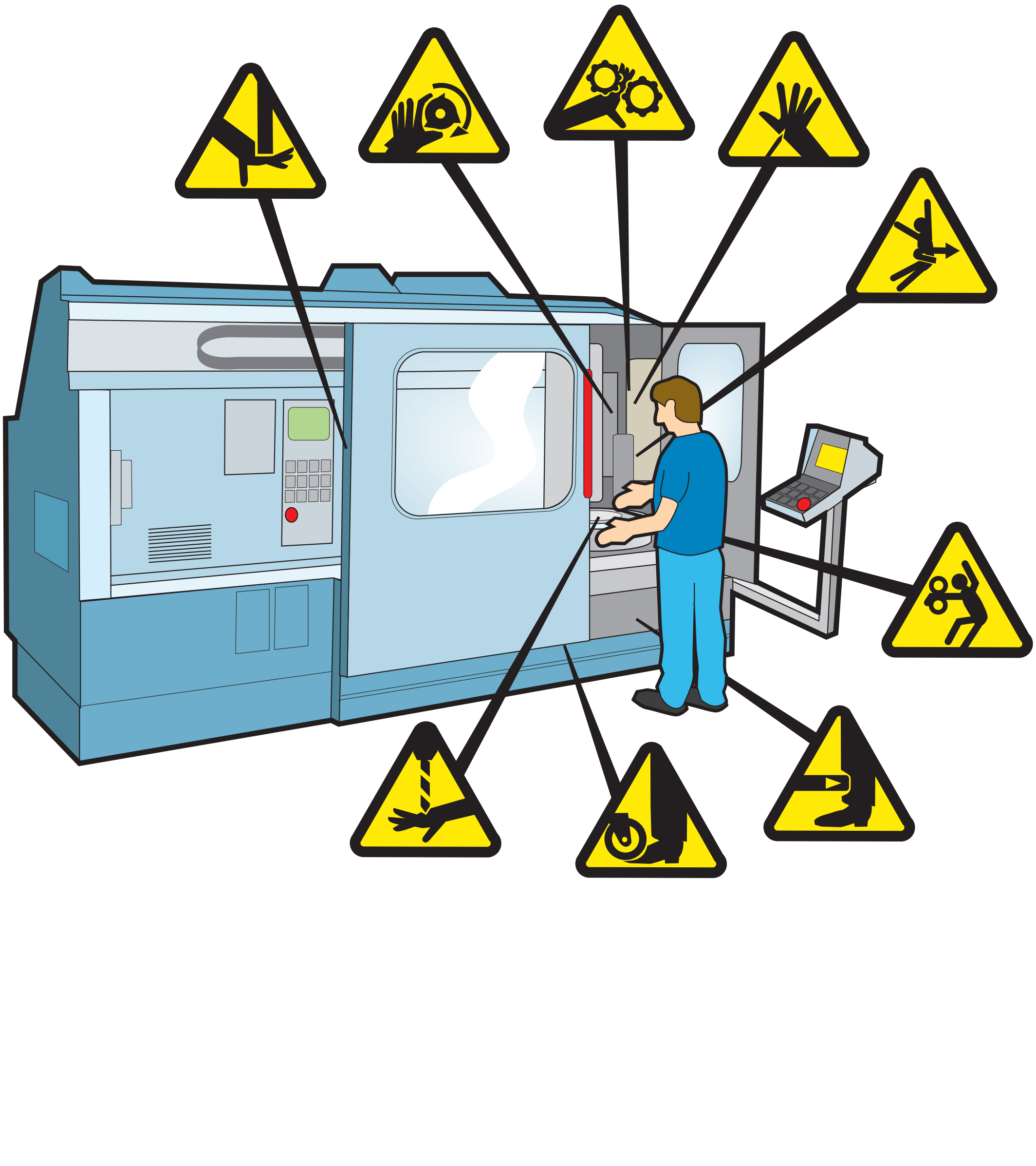
SP Technical Research Institute of Sweden

How to design safe machine control systems – a guideline to EN ISO 13849-1

Johan Hedberg
Andreas Söderberg
Jan Tegehall



SP Electronics
SP REPORT 2011:81

How to design safe machine control systems – a guideline to EN ISO 13849-1

Johan Hedberg
Andreas Söderberg
Jan Tegehall

Abstract

The aim of this report is to give guidance when applying EN ISO 13849-1:2008 in projects, both for companies developing subsystems and for companies that are developing complete machines.

The report will give support in different areas in EN ISO 13849-1:2008 that are difficult to understand or parts that are described briefly.

This report shall be considered as an complement to the standard EN ISO 13849-1:2008 that gives examples on how different requirements can be interpreted.

Key words: ISO 13849-1, IEC 62061, IEC 61508, PL, SIL, safety function, functional safety, control system.

SP Sveriges Tekniska Forskningsinstitut
SP Technical Research Institute of Sweden

SP Rapport 2011:81
ISBN 978-91-87017-14-8
ISSN 0284-5172

Borås 2011

Table of Contents

Table of Figures

Preface

The background to this report is that new standards in the area of machine control systems are more extensive compared to earlier standards, as for instance EN 954-1:1996, and the industry needs guidance concerning how to work with these new standards and how to comply with the requirements when designing systems.

This report gives a general guidance concerning how to apply EN ISO 13849-1:2008 and also describes more in detail a number of important aspects that need more detailed descriptions as for instance:

- management of functional safety
- risk assessment
- categories and designated architectures
- diagnostic coverage
- software design
- determination of reached PL (Performance Level)

Please obtain the full text of thestandard to know all parts of the standard. Standards are protected by copyright and can be bought from ISO (www.iso.org) or your national standardisations (e.g. www.sis.se in Sweden).

Summary

The aim of this report is to give guidance when applying EN ISO 13849-1:2008 in projects, both for companies developing subsystems and for companies that are developing complete machines.

The report will give support in different areas in EN ISO 13849-1:2008 that are difficult to understand or parts that are described briefly.

The first part of the report gives some general information about the new EU machinery directive 2006/42/EG.

The following part of the report is focused on management of functional safety which means how to maintain a high degree of safety during the different steps of the safety lifecycle, all the way from risk assessment until modifications of the safety function is done.

The next part of the report describes shortly how to perform a risk assessment and define an appropriate PL_r (Performance Level required) for each identified safety function.

A central part of EN ISO 13849-1:2008 is to choose an appropriate category for the identified safety functions. Categories were used also in the earlier machinery safety standard EN 954-1:1996. The report describes in detail the meaning of each category and also gives an example of a category 2 safety function.

The next step after the identification of an appropriate category is to determine the hardware reliability for each safety function. The report gives both background information about reliability theory and how to perform these calculations in practice.

Diagnostic coverage is another important are in EN ISO 13849-1:2008 that together with the category and $MTTF_d$ determines which PL that is possible to reach. The report gives a number of examples on how different diagnostic coverage techniques can look like.

The report also briefly discusses systematic failures, what it means and how to handle these during design and use of safety functions.

Software requirements are another area that is described in the report, where the report describes the difference between different kinds of programming languages and what it means to follow the V-model defined in EN ISO 13849-1:2008.

Finally the report describes a number of different methods to check that the PL_r is reached.

This report shall be considered as an complement to the standard EN ISO 13849-1:2008 that gives examples on how different requirements can be interpreted.

1 Introduction

1.1 Abbreviations

Table 1: Abbreviations

B_{10}	The expected time at which 10% of the population will fail
C	Duty cycle
DC	Diagnostic Coverage
DC_{avg}	Diagnostic Coverage Average
E/E/PE	Electrical/Electronic/Programmable electronic
HW	Hardware
L	Logic
MTBF	Mean Time Between Failure
MTTF	Mean Time To Failure
MTTR	Mean Time To Restoration
PFH_D	Probability of Dangerous Failure per Hour
PL	Performance Level
PL_r	Performance Level Required
P_{TE}	Probability of Transmission Error
RBD	Reliability Block Diagram
SFF	Safe Failure Fraction
SIL	Safety Integrity Level
SRASW	Safety-Related Application Software
SRCF	Safety-Related Control Function
SRESW	Safety-Related Embedded Software
SRP/CS	Safety-Related Part of a Control System
SRS	Safety Requirements Specification
SW	Software
TE	Test Equipment

1.2 The EU machinery directive and control systems

All machines that are used within the EU and EES area shall fulfil the EU machinery directive. Common rules in the different countries makes it easier to know which essential health- and safety requirements to be followed. The machinery directive has been reworked and the new version is valid from the 29th of December 2009.

The safety of control systems is described in Clause 1.2.1 in Appendix 1 of the machinery directive.

Control systems must be designed and constructed in such a way as to prevent hazardous situations from arising. Above all, they must be designed and constructed in such a way that:

- *they can withstand the intended operating stresses and external influences,*
- *a fault in the hardware or the software of the control system does not lead to hazardous situations,*
- *errors in the control system logic do not lead to hazardous situations,*

- *reasonably foreseeable human error during operation does not lead to hazardous situations.*

Particular attention must be given to the following points:

- *the machinery must not start unexpectedly,*
- *the parameters of the machinery must not change in an uncontrolled way, where such change may lead to hazardous situations,*
- *the machinery must not be prevented from stopping if the stop command has already been given,*
- *no moving part of the machinery or piece held by the machinery must fall or be ejected,*
- *automatic or manual stopping of the moving parts, whatever they may be, must be unimpeded,*
- *the protective devices must remain fully effective or give a stop command,*
- *the safety-related parts of the control system must apply in a coherent way to the whole of an assembly of machinery and/or partly completed machinery.*

For cable-less control, an automatic stop must be activated when correct control signals are not received, including loss of communication.

The reworked version of the machinery directive that is valid from the 29th of December 2009 does in principle have the same requirements as in the earlier version, but with the following additions:

- Predict human misbehaviour. The purpose is to reduce the risk of operational mistakes by using different kinds of ergonomic principles.
- The parameter setting of the machine is not allowed to be changed in an uncontrolled way. One example could for instance be that the processing speed of a machine is changed remotely without indicating this change to the operator of the machine.
- All safety-related parts of the machine shall work in a coherent way
- An automatic stop of the machine shall occur if no correct control signals are received via the wireless control. Loss of communication or disturbed messages shall not lead to a dangerous situation

These rules have earlier been applied in most machine control systems but now they are also specified in the machinery directive.

For certain types of machinery and logic units certain specific procedures for the CE-marking are prescribed.

If you have a machinery or a logic unit that is mentioned in Appendix 4 or 5 in the EU machinery directive, certain specific rules shall be followed to be able to fulfill the requirements. As an example, it can be necessary to use a notified body in this case.

The requirements in the EU machinery directive are intentionally written in such way to make it possible for different technical solutions. The EU machinery directive does not want to prescribe a detailed technical solution that soon can become out of date.

The EU machinery directive 2006/42/EG can be downloaded from:

http://eurlex.europa.eu/LexUriServ/site/sv/oj/2006/l_157/l_15720060609sv00240086.pdf

1.3 Reading guideline

When there are clauses, appendices, etc, mentioned in this report without explicit references, ISO 13849-1:2008 ” Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design (ISO 13849-1:2006)” is the implicit reference.

1.4 References

[1] EN ISO 13849-2 “Safety of machinery - Safety-related parts of control systems - Part 2: Validation (ISO 13849-2:2003)”

[2] EN 62061:2005 “Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems”

[3] IEC 61508:2010, Part 1 “Functional safety of electrical/electronic/programmable electronic safety related systems – Part 1: General requirements”

[4] IEC 61508:2010, Part 2 “Functional safety of electrical/electronic/programmable electronic safety related systems – Part 2: Requirements for electrical/electronic/-programmable electronic safety related systems”

[5] IEC 61508:2010, Part 3 “Functional safety of electrical/electronic/programmable electronic safety related systems – Part 3: Software requirements”

[6] IEC 61131-3:2003 “Programmable controllers – Part 3: Programming languages”

2 Management

The standard does not have a specific clause giving an overview of how to handle questions concerning management of functional safety but nevertheless it is an important part when designing a SRP/CS or a safety function. Clause 10 in the standard gives information about which documents that shall be produced during the project. Clause 4.6 “Software safety requirements” in the standard also gives some information about management, for instance that a V-model can be used when developing the software.

Both [2] and [3] contain clauses describing requirements concerning management of functional safety. When working with the standard, at least the following parts are recommended to apply:

- Develop a functional safety plan, describing:
  - Activities during the project
  - Identify persons and organisations responsible for different activities during the project
  - Competence of the persons involved in the different activities, Clause 6.2.13 and 6.2.14 in [3] give a good description
  - How to document the different steps in the project
  - Requirements when performing modification in the component/system, Clause 9 in [2] gives a good description
  - How to perform the verification (can be efficient to split up in a separate document)
  - How to perform the validation (can be efficient to split up in a separate document)
  - How to handle issues identified during for instance risk analysis, verifications, validations, audits, reviews by independent organisations, incident reporting
  - Which requirements that shall be placed on suppliers

The most important part concerning the functional safety plan is to find out how to implement it so it becomes easy to use and an integral part of the design process.

Guidance:

- It is important to early in the project to decide which documents that shall be developed by you as a manufacturer/integrator, and which documents that shall be developed by the organisation responsible for the evaluation/certification, for more information see Clause 10 in the standard
- Involve the organisation responsible for evaluation/certification as early as possible in the project. The reason for this is to detect possible deviations from the requirements in the standard as early as possible
- A general aspect for these new standards concerning functional safety is that it is not enough to design a safe system. Additionally, you must also be able to show that your system is safe by showing that you have correctly documented all parts of your development, from the initial risk analysis until the component/system is finalized

- The functional safety plan is an important document during all parts of the project life cycle and needs to continuously be updated as the project proceeds
- Documentation of good quality not only simplifies for you as a manufacturer/-integrator, but also for the organisation responsible for the evaluation/-certification. In some situations, for instance when a company does not already have existing procedures it may be efficient to build up the document structure in accordance with the clauses and requirements as described in the standard
- If possible, it is preferable to integrate the process requirements from the standard into the normal processes of the company to avoid having two different management systems
- A problem is to follow the functional safety plan developed during the whole project and also after the project is finalized and possibly evaluated/certified by another organization, and thus it is important to design the functional safety plan in such way that it is applicable and usable
- Take into consideration if it could be efficient to use a program that handles management of functional safety

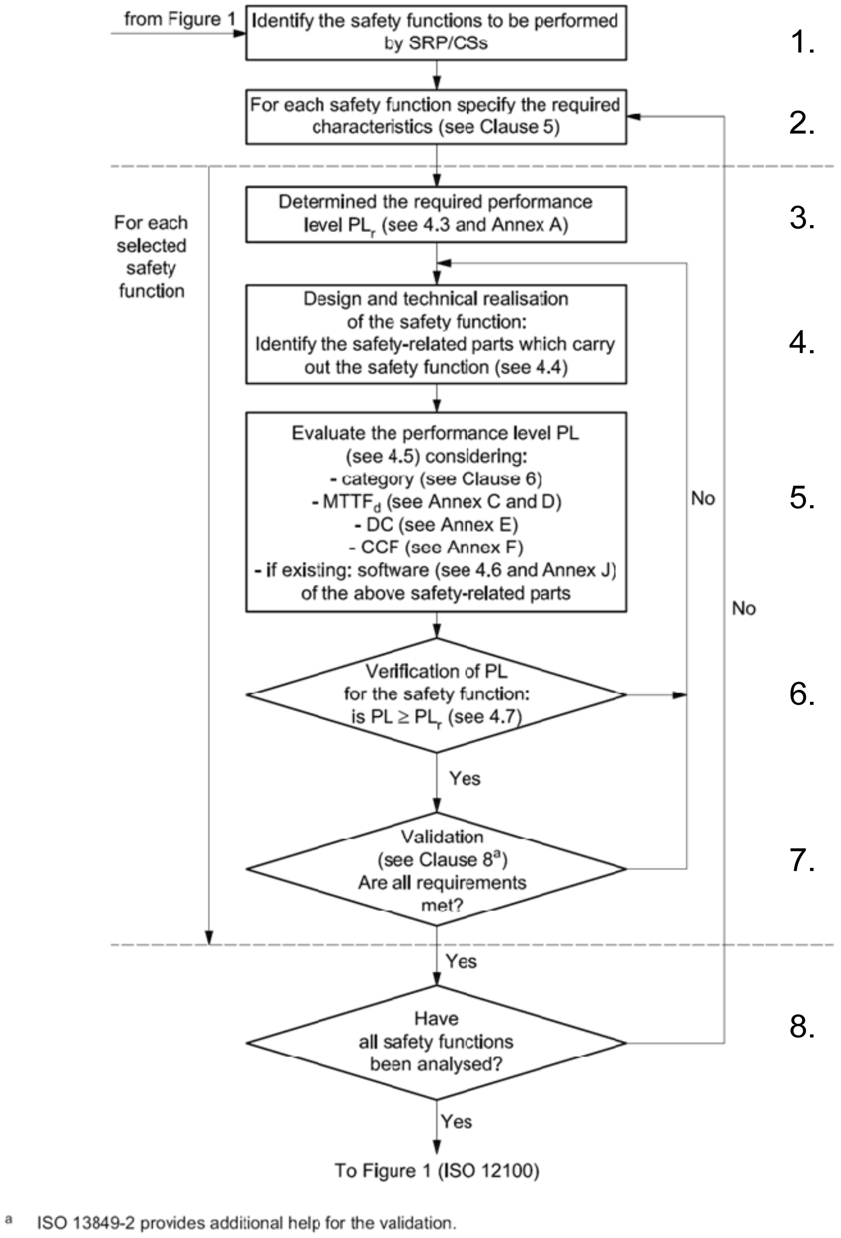

from Figure 1
Identify the safety functions to be performed by SRP/CSs
1.
For each safety function specify the required characteristics (see Clause 5)
2.
For each selected safety function
Determined the required performance level PL_r (see 4.3 and Annex A)
3.
Design and technical realisation of the safety function: Identify the safety-related parts which carry out the safety function (see 4.4)
4.
Evaluate the performance level PL (see 4.5) considering: - category (see Clause 6) - $MTTF_d$ (see Annex C and D) - DC (see Annex E) - CCF (see Annex F) - if existing: software (see 4.6 and Annex J) of the above safety-related parts
5.
No
No
Verification of PL for the safety function: is $PL \geq PL_r$ (see 4.7)
6.
Yes
Validation (see Clause 8[a]) Are all requirements met?
7.
Yes
Have all safety functions been analysed?
8.
Yes
To Figure 1 (ISO 12100)
[a] ISO 13849-2 provides additional help for the validation.

Figure 1 The safety function workflow from ISO 13849-1

Figure 3 in the standard (see Figure 1 above) describes the work flow from identifying that a safety function shall be performed by SRP/CS until the safety function has been validated. The following text describes which activities and documents that shall be performed and produced for each step.

1.
This is the result of the risk assessment / risk reduction described in Figure 1 in the standard
Documentation: List of all safety functions performed by SRP/CS. For more information see Chapter 3 in this report.

2. & 3.

The aim of this part is to more in detail describe the characteristics of each safety function. This part is important both because it is the input to the design and technical realisation, but also used as input when performing the validation of each safety function. Chapter 5.1 in the standard informs about the minimum information that shall be considered when defining the safety requirements for each safety function. Chapter 5.2 in the standard describes more in detail the safety requirements for certain safety functions.

Annex A in the standard gives an example of how to determine the required performance level (PLr) for each safety function.

The following “Requirements on requirements” are suitable to take into consideration when developing the safety requirements specification documentation.

- *Unique* – only one requirement exists addressing a specific aspect
- *Atomic* – the requirement addresses one aspect. This also improves the possibility of modifications (less dependences with other requirements)
- *Complete* – within the scope of the individual requirement
- *Unambiguous* – no room for different interpretations
- *Identifiable* – can be uniquely referenced
- *Correct* – shall address what is intended
- *Concise* – a focussed formulation
- *Verifiable* – e.g. by using tests, analysis, inspection, proofs etc.
- *Traceable* – both to upper and lower level requirements
- *Understandable* – i.e. anybody can understand the requirement. This might be somewhat in conflict with Concise.
- *Rationale* – a motivation for the requirement. This is necessary since this will improve the understanding of the individual requirement as well as groups of requirements.

Guidance:

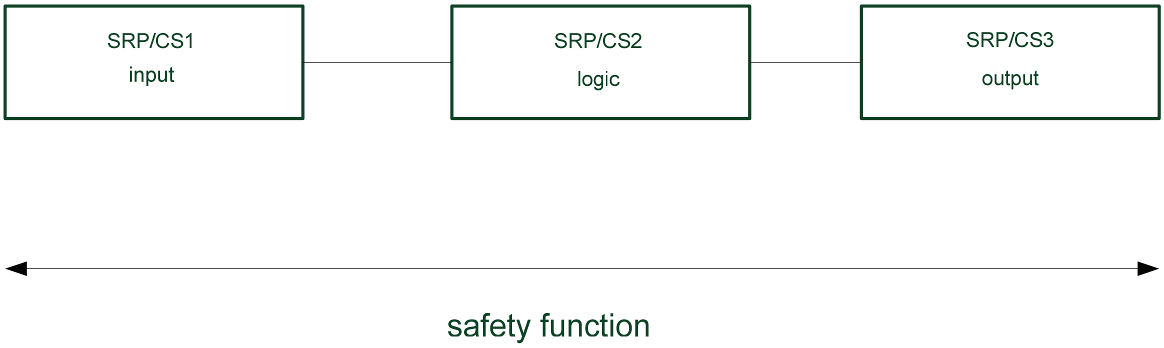
- For companies developing only a SRP/CS, the safety requirements specification will look different compared to a company developing a complete safety function, for instance:
    - The PLr will be based on a judgment of the market expectations.
    - It will only include requirements on the specific SRP/CS and not for the complete safety function.
- The safety requirements specification shall describe the functional requirements for each safety function, and thus it is important to not include any implementation-specific requirements.
- The quality of the safety requirements specification will be increased if a number of persons with different competences are included in the work, for instance persons working with development, service and quality issues. Another efficient

method is to let someone who has not been involved in the development of the document review the safety requirements specification.

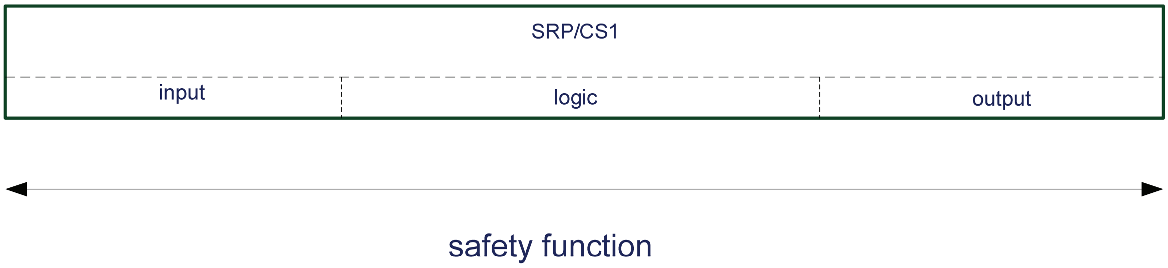
- Check the "Requirements on requirements" when developing the safety requirements specification document
- Motivate how each risk parameter is chosen in Figure A.1 — "Risk graph for determining required PLr for safety function" in the standard. For more information see Chapter 3.
- Go through Chapter 5.1 and 5.2 in the standard to get guidance concerning which information that shall be included in the safety requirements specification
- When the safety requirements specification documentation is ready, it is possible to start writing the safety validation plan, which describes how each specific requirement in the safety requirements specification will be validated.

4.

This phase concerns the design and technical realisation of the safety functions. A safety function is normally built up by a number of SRP/CSs, where each SRP/CS separately includes input, logic and output as described below:



But in some cases both input, logic and output can be integrated in the same SRP/CS as described below:



Guidance:

- It is important to identify which SRP/CSs that are included in each safety function
- A rule of thumb is if a fault in the SRP/CS will lead to a failure of the safety function then the SRP/CS shall be included as part of the safety function

- At this high level description of the safety function it will be built up by a number of SRP/CSs combined in serial.
- In some situations, the safety functions can be more complicated and for instance include two different input SRP/CSs.

5.
When all safety functions and their corresponding SRP/CSs are identified, the next step is to go on with the design of the safety function. The standard describes that the following issues are important to consider:
The PL of the SRP/CS shall be determined by the estimation of the following aspects:

- the MTTFd value for single components (see Annexes C and D in the standard)
- the DC (see Annex E in the standard)
- the CCF (see Annex F in the standard)
- the structure (see Clause 6 in the standard)
- the behaviour of the safety function under fault condition(s) (see Clause 6 in the standard)
- safety-related software (see 4.6 and Annex J in the standard)
- the ability to perform a safety function under expected environmental conditions.
- systematic failure (see Annex G in the standard)

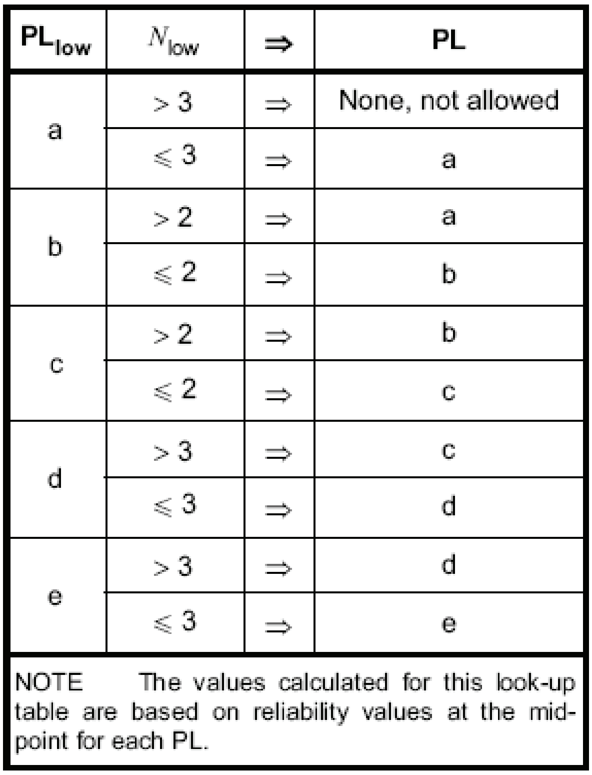
A systematic failure is a failure built in the design e.g. design mistakes. In order to reduce the possibility for design mistakes Annex G presents measures for:

- the control of systematic failures
- avoidance of systematic failures and
- avoidance of systematic failures during SRP/CS integration.

The aim with these measures are to support the design process of a SRP/CS in order to reduce the probability for systematic failures for example measures for controlling the effects of voltage breakdown, voltage variations, overvoltage and under voltage.

Chapter 6.3 in the standard describes an alternative way of calculating the reached PL for a safety function when only the PL is known for each SRP/CS. This method is described in Table 11 in the standard and also in Chapter 9.3 in this report.

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

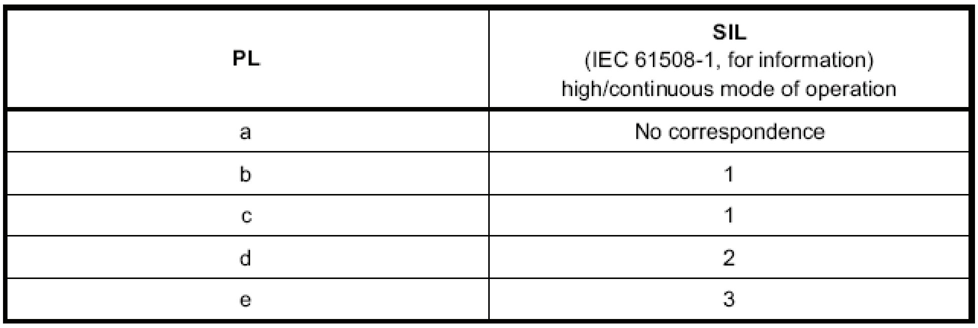


PL_{low}	N_{low}	⇒	PL
a	> 3	⇒	None, not allowed
	⩽ 3	⇒	a
b	> 2	⇒	a
	⩽ 2	⇒	b
c	> 2	⇒	b
	⩽ 2	⇒	c
d	> 3	⇒	c
	⩽ 3	⇒	d
e	> 3	⇒	d
	⩽ 3	⇒	e

NOTE The values calculated for this look-up table are based on reliability values at the mid-point for each PL.

Another usual situation for a machine builder is that the control system used in the safety function is developed according to [3], [4], [5]. In this case it is possible to check in Table 4 in the standard and transform the SIL level for the control system to a corresponding PL.

Table 4 — Relationship between performance level (PL) and safety integrity level (SIL)



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

Guidance:

- The simplified method in Chapter 4.5.4 in the standard can only be used if the architecture of the safety function corresponds to one of the designated architectures.
- The approach when using the simplified method is to first choose a certain designated architecture and then go on with the calculations of $MTTF_d$ and DC_{avg}. If the PL_r is not reached, it is possible to change the designated architecture and/or change $MTTF_d$ and/or change the DC_{avg}.

- If the PL for each SRP/CS is known, it is possible to use Table 11 in the standard to determine the PL for the safety function. In this case it is important to consider the interfaces between these different SRP/CSs and check in the safety manuals for each SRP/CS how it shall be connected to other SRP/CS.
- For other architectures, it is instead possible to apply the methods described in [4] when performing the hardware reliability calculations.

3 Risk assessment

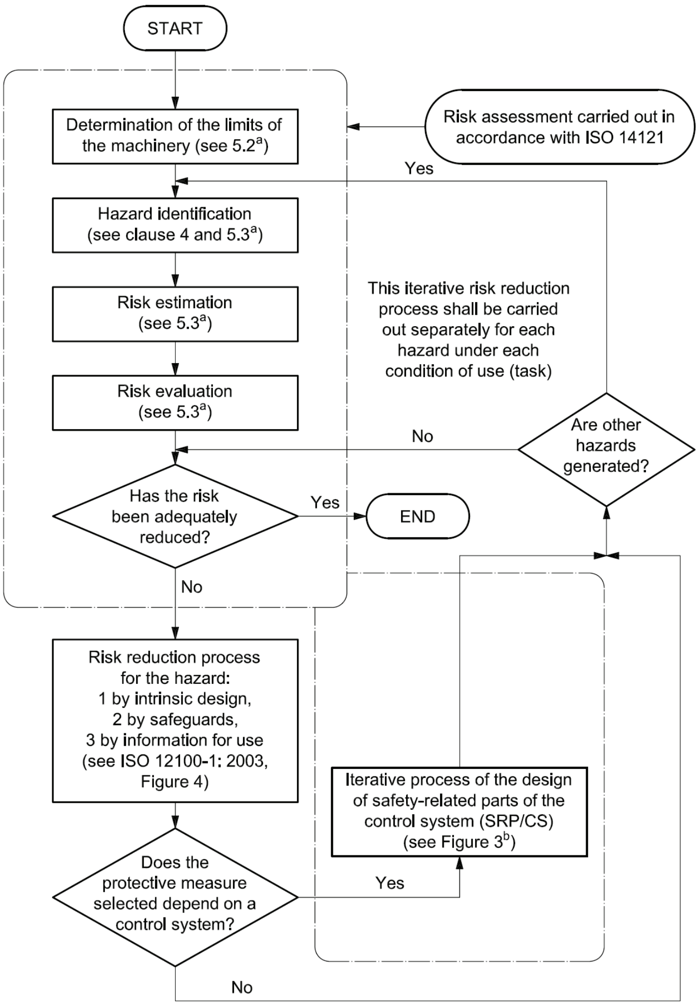
The risk assessment is performed by the manufacturer of the complete machine. The reason for this is that it is only the manufacturer of the complete machine that has got knowledge about which risks that comes with the use of the machine, and in which environment the machine shall be used.

For a manufacturer of a certain SRP/CS, a suitable PL can be found by checking the expectation from the market.

The aim of the risk assessment is to:

- Identify hazards
- Identify which hazardous events that could be connected to each hazard
- Determine whether a risk reduction is necessary or not
- Determine how the required risk reduction shall be reached
  - Identification of safety functions
  - Determination of PL_r

Below, Figure 1 from the standard describes the work flow during the risk assessment.


START
Determination of the limits of the machinery (see 5.2a)
Risk assessment carried out in accordance with ISO 14121
Yes
Hazard identification (see clause 4 and 5.3a)
Risk estimation (see 5.3a)
This iterative risk reduction process shall be carried out separately for each hazard under each condition of use (task)
Risk evaluation (see 5.3a)
No
Are other hazards generated?
Has the risk been adequately reduced?
Yes
END
No
Risk reduction process for the hazard: 1 by intrinsic design, 2 by safeguards, 3 by information for use (see ISO 12100-1: 2003, Figure 4)
Iterative process of the design of safety-related parts of the control system (SRP/CS) (see Figure 3b)
Does the protective measure selected depend on a control system?
Yes
No

[a] Refers to ISO 12100-1:2003.

[b] Refers to this part of ISO 13849.

Figure 2 The risk assessment workflow

Chapter 4.1, 4.2 and 4.3 in the standard describes in detail which requirements that are placed on the risk assessment. The next step after the identification of the hazards and the corresponding hazardous events is to decide which safety functions to be included and corresponding PL$_r$.

In the standard, five different risk reduction levels (Performance Levels) are defined, from PLa to PLe, where PLe gives the highest risk reduction and Pla gives the lowest risk reduction. For more information, see below Table 3 from the standard:

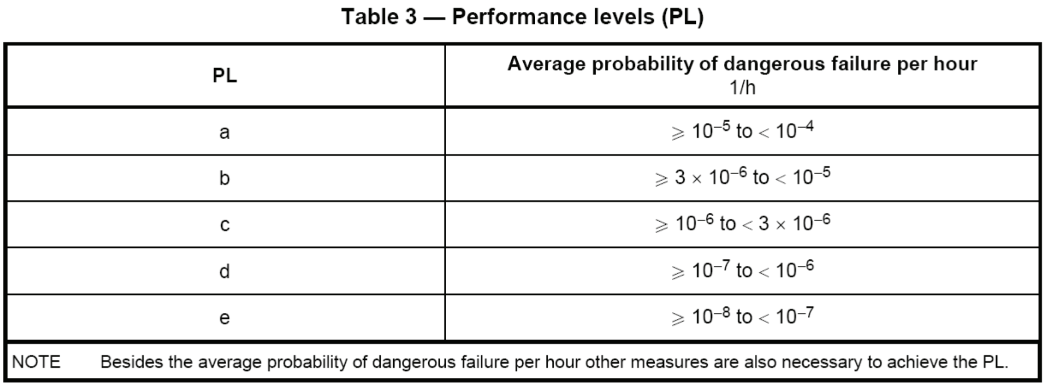
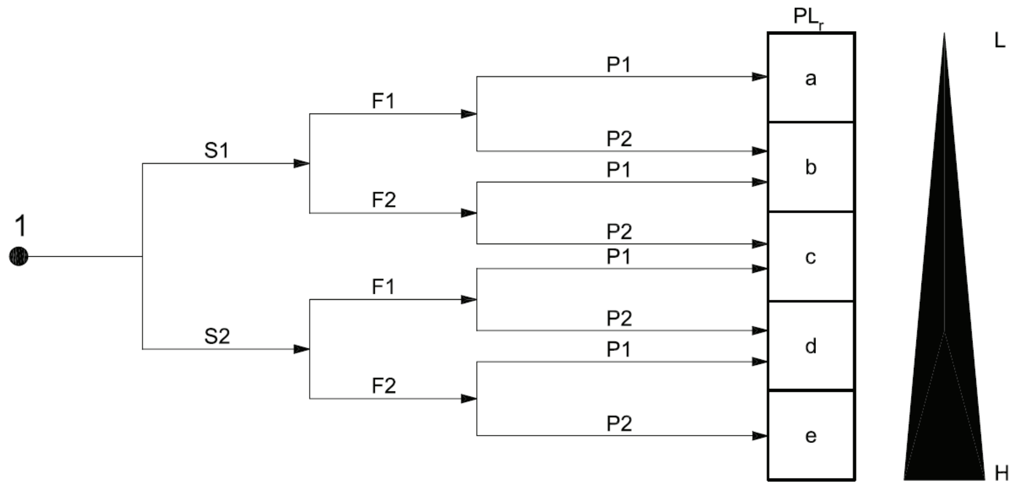


Table 3 — Performance levels (PL)

PL	Average probability of dangerous failure per hour 1/h
a	$\geqslant 10^{-5}$ to $< 10^{-4}$
b	$\geqslant 3 \times 10^{-6}$ to $< 10^{-5}$
c	$\geqslant 10^{-6}$ to $< 3 \times 10^{-6}$
d	$\geqslant 10^{-7}$ to $< 10^{-6}$
e	$\geqslant 10^{-8}$ to $< 10^{-7}$
NOTE Besides the average probability of dangerous failure per hour other measures are also necessary to achieve the PL.	

Figure A.1 in the standard can be used when deciding an appropriate risk reduction level:



Key

1 starting point for evaluation of safety function's contribution to risk reduction

L low contribution to risk reduction

H high contribution to risk reduction

PL$_r$ required performance level

Risk parameters:

S severity of injury

S1 slight (normally reversible injury)

S2 serious (normally irreversible injury or death)

F frequency and/or exposure to hazard

F1 seldom-to-less-often and/or exposure time is short

F2 frequent-to-continuous and/or exposure time is long

P possibility of avoiding hazard or limiting harm

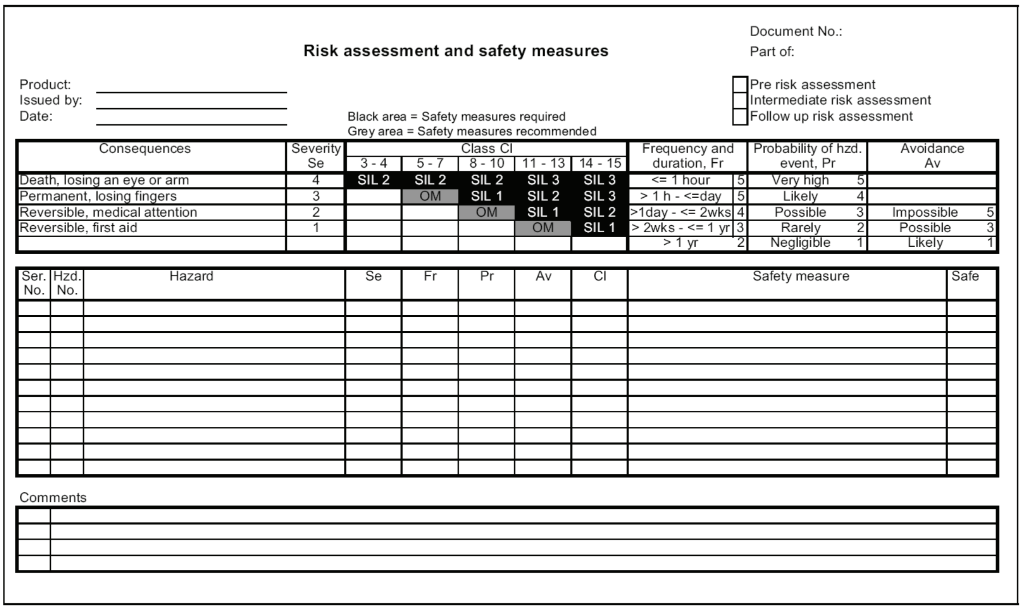
P1 possible under specific conditions

P2 scarcely possible

Figure A.1 — Risk graph for determining required PL$_r$ for safety function

Figure 3 ISO 13849-1 Figure A.1– Risk graph

Figure A.1 in the standard is a simple method to determine the PL_r for a safety function. One disadvantage with this risk graph is that it does not take into consideration the frequency of the hazardous events. In this case one possibility is to instead use the risk graph matrix described in Figure A.3 in [2].



Document No.:

Risk assessment and safety measures

Part of:

Product: ____________
Issued by: ____________
Date: ____________

□ Pre risk assessment
□ Intermediate risk assessment
□ Follow up risk assessment

Black area = Safety measures required
Grey area = Safety measures recommended

Consequences	Severity Se	Class Cl					Frequency and duration, Fr		Probability of hzd. event, Pr		Avoidance Av	
		3 - 4	5 - 7	8 - 10	11 - 13	14 - 15						
Death, losing an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	<= 1 hour	5	Very high	5		
Permanent, losing fingers	3		OM	SIL 1	SIL 2	SIL 3	> 1 h - <=day	5	Likely	4		
Reversible, medical attention	2			OM	SIL 1	SIL 2	>1day - <= 2wks	4	Possible	3	Impossible	5
Reversible, first aid	1				OM	SIL 1	> 2wks - <= 1 yr	3	Rarely	2	Possible	3
							> 1 yr	2	Negligible	1	Likely	1

Ser. No.	Hzd. No.	Hazard	Se	Fr	Pr	Av	Cl	Safety measure	Safe

Comments

Figure A.3 – Example proforma for SIL assignment process

Figure 4 Risk graph matrix

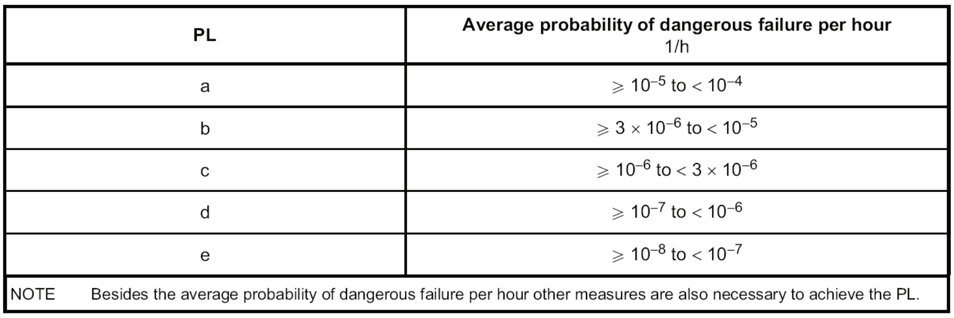
Figure A.3 in [2] (Figure 4 above) gives as result that the safety function shall fulfill a certain SIL, and thus it is necessary to transform this SIL value into a PL_r value and this is possible by first using Table 3 in [2] to check which PFH_D interval that corresponds to each SIL.

Table 3 – Safety integrity levels: target failure values for SRCFs

Safety integrity level	Probability of a dangerous Failure per Hour (PFH_D)
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

And then check by using Table 3 in the standard which PL_r that corresponds to each PFH_D.

Table 3 — Performance levels (PL)



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

NOTE Besides the average probability of dangerous failure per hour other measures are also necessary to achieve the PL.

By combining these tables it is possible to say **from a risk assessment view** that:

- SIL 3 corresponds to PL_r=e
- SIL 2 corresponds to PL_r=d
- SIL 1 corresponds to PL_r=c (this is a conservative approach because the probability of dangerous failure per hour interval for SIL 1 covers both PL_r=b and PL_r=c)

When performing the risk assessment outgoing from Table A.3 in [2] it is not possible to reach PLa and PLb.

4 Category and designated architectures

The categories represent resistance to hardware faults, and have previously been the most common used principle in order to design a control system that have an appropriate level of safety for the risks that are present for the intended use of the machine. The category is one of the sub requirements of a PL and there is a possibility within a PL to choose different categories.

The category is essential to take into consideration during the first design phase since the category affects both the hardware design and the software design. If the principles for the category (designated architectures) are not followed, the simplified method for calculation of hardware reliability as presented by the standard is not valid. In the case when a designated architecture is not followed, other methods for calculation of hardware reliability is possible, such as methods according to [4] (not covered by this report).

It is important to remember that in some cases some the categories is not suitable for the final application because the checking of the safety function cannot be applied to all components, see Chapter 4.1.3.1.

What is a category?
The category describes resistance to faults and the behavior of the machine or the control system in the case a fault occurs in the safety related part of a control system. The category is defined in the standard as:

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

There are five types of categories defined: B, 1, 2, 3, 4 and thus we have five different types of fault resistances defined. The category was previous (EN 954-1:1996) the measure to reduce the risk by selecting an appropriate category according to the risks analysis.

If the risk for a machine is estimated to be high, and we suppose that the result of a risk assessment gives Performance Level required (PL_r) = d for a specific safety function. The following is possible:

- category 2 or category 3 structure can be used
- category B or category 1 structure are not fulfilling requirements for PL_r = d
- category 4 structure is in this case possible but will give higher design requirements for the estimated risk according to the standard

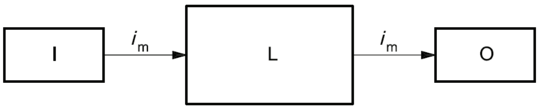
The principle for the categories (resistance to faults) is almost identical if we compare requirements from the standard and EN 954-1:1996 but $MTTF_d$, DC_{avg} and CCF need also to be considered.

4.1 Designated architectures

The designated architectures are presented by an graphical structure with boxes and arrows for each category by the standard. To be able to apply the simplified method the architecture shall be in accordance with one of these designated architectures.

4.1.1 Category B

The figure below presents the designated architecture for category B. Category B is a single channel system.



Key

i_m interconnecting means

I input device, e.g. sensor

L logic

O output device, e.g. main contactor

Figure 5. Designated architecture for category B [EN ISO 13849-1 figure 8]

The B category is mainly characterized by selection of components, the occurrence of a fault can lead to the loss of the safety function.
The B category gives "*basic requirements*", these requirements are also required for all other categories (1, 2, 3 and 4).

The requirements for category B mean that the components are suitable for the intended use with respect to:

- design, construction, selection, assembly and combination so the SRP/CS components are in accordance with relevant standards
- environmental conditions, for example temperature, vibrations, dust, moisture, humidity, water
- operating stresses, influences of materials processed and other relevant influences.
- basic safety principles see Chapter 4.1.1.1 in this report

It is not possible in general to say that a component is a category B component since the intended use and the environmental conditions give requirements on category B. The manufacturer of the component specifies technical data for the component so that the user can select a component that fulfill requirements for category B. The manufacturer of the component cannot say in general that "*category B is fulfilled*" if the final application for the component is not known.

Example* of category B solutions:

- interlock switch for a laundry machine prevents the machine to start when the door is open

* Remember that product standards or the risk assessment can give other required categories due to PL_r.

4.1.1.1 Basic safety principles

The basic safety principles give requirements for the used technology. Mechanical systems, pneumatic systems, hydraulic systems and/or electrical systems [1].

Basic safety principles are based on the following design aspects (when suitable):

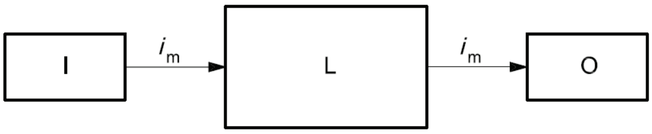
- use of suitable materials and adequate manufacturing
- correct dimensioning and shaping
- proper selection, combination, arrangements, assembly and installation of components/system
- correct protective bonding
- proper fastening
- insulation monitoring
- use of de–energisation principle
- transient suppression
- energy limitation (pressure, speed)
- reduction of response time
- compatibility
- withstanding environmental conditions
- secure fixing of input devices
- protection against unexpected start–up
- protection of the control circuit
- sequential switching for circuit of serial contacts of redundant signals
- simplification (reduce the number of components in the safety–related system)
- separation
- proper temperature range
- sufficient avoidance of contamination of the fluid
- proper range of switching time
- limitation of the generation and/or transmission of force and similar parameters
- limitation of range of environmental parameters
- proper lubrication
- proper prevention of the ingress of fluids and dust

[Summary of Table A.1, B.1, C.1 and D.1 in [1]]

When mechanical systems, pneumatic systems, hydraulic systems or electrical systems are used in conjunction with other technologies, relevant measures for basic safety principles should also be taken into account.

4.1.2 Category 1

The figure below presents a designated architecture for category 1. Category 1 is a single channel system.



Key

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

Figure 6 Designated architecture for category 1 [EN ISO 13849-1 figure 9]

The category 1 structure is mainly characterized by selection of components, the same principle as category B, and the occurrence of a fault can lead to the loss of the safety function. The probability of occurrence of a fault is lower than a category B structure in comparison.

Basic requirements of category B shall apply but in addition well-tried safety principles (see Chapter 4.1.2.1 in this report) and well-tried components (see Chapter 4.1.2.2 in this report) shall be used.

Example[*] of category 1 solutions:

- door interlock switch for a wood working machine
- emergency stop device

[*] Remember that product standards or the risk assessment can give other required categories due to PL_r.

4.1.2.1 Well-tried safety principles

Well-tried safety principles shall give a higher degree of safety in comparison with basic safety principles due to the design measures.

Well-tried safety principles are described for electrical systems, mechanical systems, pneumatic systems and hydraulic systems by [1].

Electrical systems

List of well tried safety principle for electrical systems [1]:

- positive mechanically linked contacts
- fault avoidance in cables
- separation distance
- energy limitation
- limitation of electrical parameters
- no undefined states
- positive mode actuation
- failure mode orientation
- over–dimensioning
- minimise possibility of faults
- balance complexity/simplicity

[Table D.2 in [2]

Applicable well-tried safety principles shall be adopted during the design phase and documented in order to support the validation activities. Some principles are described below:

- If we compare an "ordinary" switch with a switch that have *Positive mode actuation* the "ordinary" switch has a higher probability that the switch will not open due to a mechanical faults or welded contacts.

positive mode actuation
Direct action is transmitted by the shape (and not by the strength) with no elastic elements, e.g. spring between actuator and the contacts, (see ISO 14119:1998, 5.1, ISO 12100-2:2003, 4.5).

- Fault avoidance can be reached in cables by avoiding that short circuits between two adjacent conductors can occur. A typical measure can be a cable with shield connected to the protective bonding circuit on each separate conductor. For flat cables a measure can be one earthed conductor between each signal conductor.

All applicable well-tried safety principles shall be followed for the intended application and technology used where applicable see A.3, B.3, C.3 and D.3 in [1].

When mechanical systems, pneumatic systems, hydraulic systems or electrical systems are used in conjunction with other technologies, relevant measures for basic safety principles and well-tried safety principles should also be taken into account.

Mechanical systems
List of well tried safety principle for mechanical systems [1]:

- use of carefully selected materials and manufacturing
- use of components with oriented failure mode
- over–dimensioning/safety factor
- safe position
- increased OFF force
- carefully selection, combination, arrangement, assembly and installation of components/system related to the application
- carefully selection of fastening related to the application
- positive mechanical action
- multiple parts
- use of well–tried spring
- limited range of force and similar parameters
- limited range of speed and similar parameters
- limited range of environmental parameters
- limited range of reaction time, limited hysteresis

[Table A.2 EN ISO13849-2]

Applicable well-tried safety principles shall be adopted during the design phase and documented in order to support the validation activities.

Pneumatic systems and hydraulic systems
List of well tried safety principles for pneumatic and hydraulic systems [1]:

- Over–dimensioning/safety factor
- Safe position
- Increased OFF force
- Valve closed by load pressure
- Positive mechanical action
- Multiple parts
- Use of well-tried spring
- Speed limitation/speed reduction by resistance to defined flow
- Force limitation/force reduction
- Appropriate range of working conditions
- Proper avoidance of contamination of the fluid
- Sufficient positive overlapping in piston valves
- Limited hysteresis

[Table B.2 and C.2 in [1]]

Applicable well-tried safety principles shall be adopted during the design phase and documented in order to support the validation activities.

4.1.2.2 Well-tried component

A well-tried component shall be carefully selected and also be demonstrated that it is suitable for the intended application.

For category 1 solutions the well-tried component is a key component for safety.

Description of a well-tried component in the standard:

> A "well-tried component" for a safety-related application is a component which has been either
> a) widely used in the past with successful results in similar applications, or
> b) made and verified using principles which demonstrate its suitability and reliability for safety-related applications.

It is important to understand that the qualification of a component to be a well-tried depends on its application. If safe operation relies on a single component, it is of great importance that this component is designed and implemented for the final application by following basic and well-tried safety principles.

Remember that a well–tried component for some applications can be inappropriate for other applications.

In [1] examples of well-tried components are given for electrical systems and mechanical systems.

Electrical systems
A list of well tried components for electrical systems [1]:

- switch with positive mode actuation e.g.: push–button, position switch, cam-operated selector switch e.g. for mode of operation
- emergency stop device
- fuse
- circuit breaker
- switches, disconnectors
- differential circuit breaker/ RCD (Residual current detection)
- main contactor
- control and protective switching device or equipment (CPS)
- auxiliary contactor (e. g. contactor relay)
- relay
- transformer
- cables
- plug and socket
- temperature switch
- pressure switch
- solenoid for valve

[Table D.3 in [1]]

The aspects that influence if a component can be regarded as well-tried are:

- follow well-tried safety principles
- have low complexity and
- are demonstrated suitable by applying applicable standards.

low complexity component
component in which
– the failure modes are well-defined; and
– the behaviour under fault conditions can be completely defined
[2]

Some principles are described below:

- a switch with positive mode actuation demonstrates its suitability and reliability if the switch complies with EN 60947–5–1:1997 see [1] for details.
- a main contractor has to fulfill additional conditions in order to be regarded as "well–tried" such as over – dimensioning, see [1] for details.

Remember that the intended application affects “well-tried” components. For example cabling to external enclosure should be protected against mechanical damage (including e.g. vibration or bending) in order to be regarded as a “well-tried” component.

Complex components: Electronic components (e.g. PLC, microprocessor, application-specific integrated circuit) cannot be considered as equivalent to “well tried” since they are complex components, see the definition below.

complex component
component in which
– the failure modes are not well-defined; or
– the behaviour under fault conditions cannot be completely defined
[2]

Mechanical systems
A list of well tried components for mechanical systems [1]:

- Screw
- Spring
- Cam
- Break–pin

[Table A.3 in [1]]

Well–tried components for a safety–related application in the list above are based on the application of well–tried safety principles and/or a standard for their particular applications.

For a screw locking a mechanical cam the following requirements (table A.2 in [1]) can be applicable:

- use of carefully selected materials and manufacturing
- over–dimensioning/safety factor
- carefully selection, combination, arrangement, assembly and installation of components/system related to the application
- carefully selection of fastening related to the application

The screw shall have suitable material due to environmental conditions, correct over dimensioning due to a safety factor suitable for the application, selection/arrangement/ assembly of components that are suitable for the application and proper fastening.

A well–tried component for some applications can be inappropriate for other applications.

Pneumatic and hydraulic components
At the present time no list of well-tried pneumatic and hydraulic components are given. The status of being well-tried is mainly application specific. A well-tried component for some applications can be inappropriate for other applications.

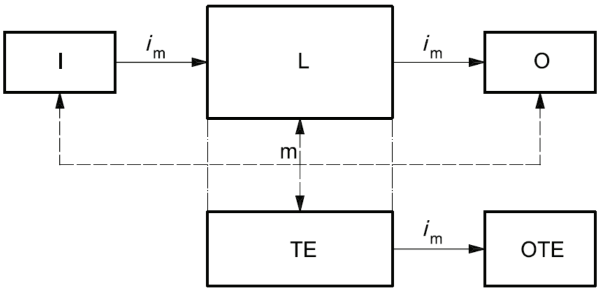
Summary regarding well-tried components:

- Applicable basic safety principles according to category B shall be followed.
- Well–tried components for a safety–related application are based on the application of well–tried safety principles and/or a standard for their particular applications.
- Intended use shall not affect the well-tried component e.g. environmental conditions
- A well–tried component for some applications can be inappropriate for other applications.
- A well tried component is a low complex component
- Category 1 is the only category that requires well tried components. Category 1 components can be used in category 2, 3 and category 4 systems. In this case the total resistance to faults and the subsequent behavior in the fault condition shall be according to the intended category (2, 3 or 4).

4.1.3 Category 2

A designated architecture for category 2 is presented by the standard. Category 2 is not a single channel system. Basic requirements of category B shall apply and were applicable, well-tried safety principles shall be used.

Category 2 has an additional test equipment (TE) that test and monitors (dashed arrows) Input, Logic and Output with a periodic test interval. The occurrence of a fault can lead to the loss of the safety function between the checks.



Dashed lines represent reasonably practicable fault detection.

Key

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

Figure 7 Designated architecture for category 2 [EN ISO 13849-1 figure 10]

The periodic test interval is depending on the application, the checking interval shall be as short as possible, I, L and O shall be checked/ monitored. All "boxes" of the designated category 2 architecture need a corresponding hardware unit.

The checking interval can be time scheduled or based on the operating cycle or the machine cycle. It is important that the interval is suitable for application. The checking interval needs to be evaluated/determined during the risk assessment for the application.

The Output of Test Equipment (OTE) needs to be separated/independent from the Output (O).

An example of O and OTE components:

- Relay
- Contactor
- Transistor

Example* of category 2 solutions:

- Force limitation system for a overhead sectional industrial door

* Remember that product standards or the risk assessment can give other required categories due to PL_r.

4.1.3.1 Disadvantage with a category 2 solution

A category 2 system is a mixture of a category B or 1 and a category 3 system since input is only one sensing unit and output is two separate units.

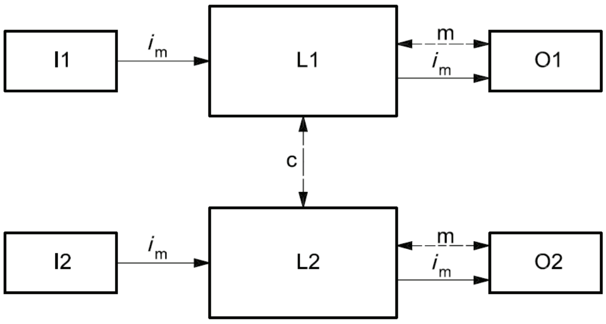
In some applications category 2 is difficult to realize since some of the components (I, L or O) may not be checked periodically. In this case a category 3 system may be more suitable since a category structure 3 is based on two independent hardware channels with comparison/monitoring of the two channels.

4.1.4 Category 3

Category 3 is a redundant system with monitored inputs and outputs (with other words a two channel system that has monitoring of inputs and outputs). This means that we have a single fault tolerant system with diagnostics.

Basic requirements of category B shall apply and applicable well-tried safety principles shall be used.

A designated architecture for category 3 is presented in the standard.



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

Figure 8 Designated architecture for category 3 [EN ISO 13849-1 figure 11]

Some faults are not detected by a category 3 system; these faults shall have a motivation why they are not detected. All "boxes" of the designated category 3 architecture need a corresponding hardware unit.

Inputs (I1 and I2) are checked so that discrepancies are detected. When a discrepancy is detected, action is taken to reach a safe state.

Logic (L1 and L2) are checked so that discrepancies are detected. When a discrepancy is detected, action is taken to reach a safe state.

Outputs (O1 and O2) are checked so that discrepancies are detected. When a discrepancy is detected action is taken to reach a safe state.

Example* of category 3 solution(s):

- Input circuit for an interlock door for Machinery. The I1 and I2 are two separate electric channels of one electro-mechanic door key switch with positive mode of operation. The switch has two electrical channels but only one mechanical channel (the key). Mechanical faults are in this case excluded since this component is regarded as well tried due the mechanical design and the contact elements I1 and I2 have positive mode of operation.

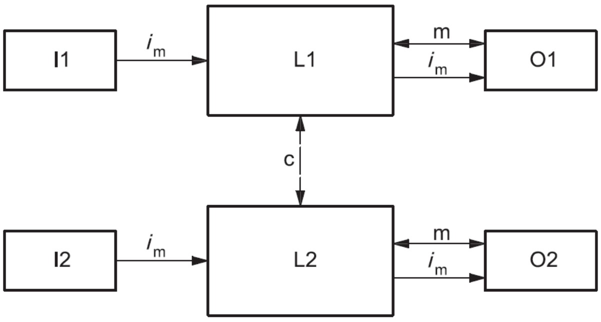
* Remember that product standards or the risk assessment can give other required categories due to PL_r.

4.1.5 Category 4

Category 4 is a redundant system with monitored inputs and outputs (with other words a two channel system that has monitoring of inputs and outputs). Single faults does not lead to loss of safety function and accumulation of undetected faults shall not lead to the loss of the safety function. Category 4 offers a higher degree of resistance to faults in comparison with category 3.

Basic requirements of category B shall apply and applicable well-tried safety principles shall be used.

A designated architecture for category 4 is presented in the standard.



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

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

Figure 9 Designated architecture for category 4 [EN ISO 13849-1 figure 12]

The accumulation of two faults is considered to be sufficient in the standard:

The difference between category 3 and category 4 is a higher DCavg in category 4 and a required MTTFd of each channel of “high” only. In practice, the consideration of a fault combination of two faults may be sufficient

Inputs (I1 and I2) are checked so that discrepancies are detected. When a discrepancy is detected action is taken to reach a safe state.

Logic (L1 and L2) are checked so that discrepancies are detected. When a discrepancy is detected action is taken to reacha safe state.

Outputs (O1 and O2) are checked so that discrepancies are detected. When a discrepancy is detected action is taken to reacha safe state.

Example* of category 4 solution(s):

- Input circuit for an interlock door for Machinery. The I1 and I2 is two separate electro mechanic door key switches. They each key switch have one electrical channel and one mechanical channel (key) each. Mechanical faults are in this case not excluded since the combination of two separate electro mechanical switches achieves category 4.

* Remember that product standards or the risk assessment can give other required categories due to PL_r.

4.2 Important issues during the design phase

The category principles are important to verify early in the design process. The first step is to ensure that all of the “boxes” are represented for the target category. The arrows need an functional representation.

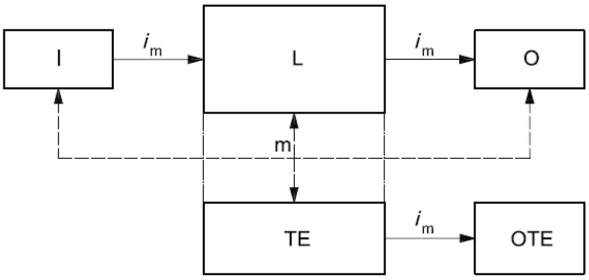


Figure 10 A category 2 structure

When a category 2 structure is used
All of the “boxes” Input (I), Logic (L), Output (O), Test Equipment (TE) and Output Test Equipment (OTE) need a representation by a hardware (HW) unit. All boxes shall be identified and described.

The monitoring of I, L and O (dashed arrows) needs to be identified and described. If the monitoring is not fulfilled the DC_{avg} calculations will probably fail.
Example If no feedback exists from output (O) the DC_{avg} for the output is 0% . Lack of feedback will probably get too low DC_{avg} for the calculations for the complete safety function.

4.2.1 Example – Category 2 force limitation system

In order to protect people from harm on a overhead sectional industrial door, a force limitation system (PSPE Pressure Sensitive Protective Equipment) is required. The manufacturer of the control system aims to design the force limitation system according to category 2.

Force limitation system for a overhead sectional industrial door
When the door moves downwards there are crushing hazards between the door leaf and the ground. In order to prevent crushing hazards, the door reverses the direction of movement if the door leaf hits an obstacle (the safety edge is affected).

Identification of HW units:

I	=	Safety edge (Pressure sensitive protective device)
L	=	Control unit with a micro controller
O	=	Motor driver

TE = Separate watchdog system
OTE = A relay that de-energizes the motor diver (O)

Description of safety measures for Input (I)
The input interface (i_m between I and L) is checked before the start of the motor. In the event of a fault, the door is not started on the start impulse.
Once per door cycle (opening and closing of the door leaves) the safety edge hits the ground. If no there is reaction from the safety edge (I) when the door leaf hits the ground, the door is stopped by over current detection, In this case a faulty safety edge is detected and further automatic operation of the door is prohibited.

Description of safety measures for Logic (L)
The Logic has internal tests in order to ensure safe and reliable operation. These tests are based on the DC table for logic in Annex E of the standard.

- Inputs are tested periodically
- Static and dynamic memories are checked periodically
- Program execution is monitored
- Power failure is monitored in order to ensure safe operation
- I/O stuck at faults are monitored
- Watch dog
- Outputs are tested

These internal tests are necessary for applications where the manufacturer develops electronic safety critical systems, for example when developing safety critical embedded systems based on commercial on the shelf microprocessor(s).

Logic units such as Safety – PLC, Safety Relay or Safety Controllers (certified according to the standard or [3], [4] and [5] has from factory implemented internal self tests. For these units it is necessary to follow factory recommendations and implement these logic controllers (for example verify the application program and the parameterization software) according to the risks for the final solution.

Description of safety measures for Test Equipment (TE)
Test equipment is an independent unit that monitors, logic, input and output in order to ensure reliable and safe operation.

Description of safety measures for Output (O)
The motor driver (O) is tested that it is able to operate before start of the door, a simulated deactivation of the motor driver is done and a check is made that the motor does not operate. In the event that a fault is detected further automatic operation of the door is prohibited. If the motor does not stop the door in the event of a stop command, the relay (OTE) de-energizes the motor driver (O).

The feedback from the motor is based on two independent sources, motor current and encoder signal.

Description of safety measures for Output Test Equipment (OTE)
The OTE relay de-energizes the motor driver (O) in the event when the motor driver does not de-energize the motor.

5 Probability of dangerous failures

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

Aim
To give a short introduction in the concept of MTTFd, how to retrieve MTTFd-values for components and how to estimate the total MTTFd for a SRP/CS.

Requirements
The MTTFd is given in three levels and shall be taken into account for each channel of the SRP/CS individually

Denotation of each channel	Range of each channel
Low	3 years ≤ MTTFd < 10 years
Medium	10 years ≤ MTTFd < 30 years
High	30 years ≤ MTTFd < 100 years

A channel can have a MTTFd maximum value of 100 years. If the estimation results in a channel with a MTTFd > 100 years, the resulting MTTFd is set to 100 years.

The following sub-chapters are guidance.

5.1 MTTF$_d$

5.1.1 Basic definitions

One of the main differences between thestandard and the earlier EN 954-1:1996 is the addition of hardware reliability requirements. All hardware components has a probability of failure per unit time, this probability is called the component failure rate and is denoted with the symbol λ (lambda). Failure rate is often estimated in failures in time (FIT) which means that if a component has a failure rate of 1 FIT then the probability of failure for that component is 1×10^{-9} per hour.

The failure rate for a certain type of component can be subdivided into three phases according to the following figure:

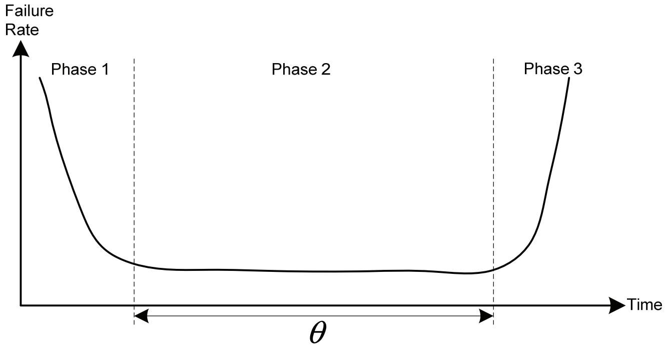


Figure 11 Bathtub curve

Phase 1 is the early life of the component. During this period the failure rate is expected to be high because of e.g. a not sufficiently adjusted manufacturing process.

During phase 2 the failure rate is assumed to be constant for electric/electronic, hydraulic and pneumatic components. This period is called the useful life of the component which often is symbolized with θ (theta).

Phase 3 is the wear out phase which starts when the useful life of the component ends. In this phase the component is worn out because of physical reasons and the failure rate cannot longer be assumed to be constant.

Because the failure rate is assumed to be constant during the useful life period it can be shown that the mean time to failure (MTTF) can be calculated according to:

$$MTTF = \frac{1}{\lambda}[hours]$$

It is very important to make a difference between the MTTF and the θ because these two measures have no relationship. For example, wet electrolytic capacitors often has a limited θ because of drying in time. However before the end of θ these capacitors usually has a very low failure rate and thus a very large MTTF.

Sometimes the term MTTF is confused with the term MTBF (mean time between failures). According to reliability theory literature MTBF is defined as follows:

$$MTBF = MTTF + MTTR$$

Where MTTR means: mean time to repair and is a measure of the expected time to successfully repair a component/system. Usually MTTR << MTTF (e.g. 8 hours compared with 3500 years). The term MTBF is normally important in maintainability/availability analysis and will not be further considered in this report.

5.1.2 Relation between MTTF and MTTFd

Example

Consider a relay with one contact supplying a motor. The failure rate for the relay is known (λ_{RE}). The relay has two failure modes, stuck open or stuck closed and the relay manufacturer has specified that if a relay failure occurs, it is equally probable that any of these failure modes occur. This is called distribution of the failure rate among the failure modes of a component. Reliability prediction handbooks may provide guidance for distribution for certain types of components (but not for all types) if not the distribution is carried out by good engineering practice.

FMEA – Example motor control

Failure mode	**Failure effect**	**Fraction of failure rate**
Stuck-open	The motor cannot start, or stops unexpectedly	Safe failure effect $= 50\% \cdot \lambda_{RE}$
Stuck close	Unexpected start, or the motor does not stop	Dangerous failure effect $= 50\% \cdot \lambda_{RE}$

In a realistic case, there would be a lot more components in the FMEA. When the FMEA is completed the total failure rate leading to safe failure effects is added together. This total failure rate is denoted with the symbol λ_S (safe failure rate) and the total failure rate leading to dangerous failure effects is denoted with the symbol λ_D (dangerous failure rate) where:

$$MTTF_D = \frac{1}{\lambda_D}[years]$$

When estimating MTTFd for a component the following procedure for finding data shall be followed according to Clause 4.5.2 in the standard:

a) Use manufacturers data
b) Use methods in Annexes C and D in the standard
c) Choose ten years

5.1.3 Estimation of MTTFd for electric/electronic components

There are different techniques to estimate the failure rate for components, either the failure rate is determined by counting failures in the field on a large population of components, and then use statistical methods (which is the most accurate method) or the failure rate is predicted using a reliability prediction handbook.

Always check if the manufacturer specifies the MTTFd value in the component datasheet. In some cases the datasheet only contains a PFH value or a λ_D value (this is common for electronic modules such as I/O modules and sensors). In this case use the formula MTTFd = $1/\lambda_D$
However, for standard passive components (transistors, diodes, resistors etc.) use the following guideline:

The latter technique is the most common for electronic components. Annex C in the standard give reliability figures for most discrete electronic components and may be used unless the component manufacturer provides reliability data. For complex components (integrated circuits) consult a reliability expert who can help predicting failure rates.

Example from Table C.2 in the standard Bipolar transistor which is assigned with the following values:
MTTF = 34247 years
MTTFd (typical) = 68493 years
MTTFd (worst case) = 6849 years

For each electronic component in Annex C in the standard it is assumed that 50% of all the component failure modes leads to a dangerous failure providing the typical MTTFd:

$$MTTFd = 2 \times MTTF \; (\lambda_D = 0.5 \times \lambda = \frac{1}{2}\lambda \Rightarrow \frac{1}{MTTFd} = \frac{1}{2 \times MTTF}).$$

For each component there is also provided a worst case MTTFd where a safety margin of a factor 10 have been used.

As far as possible select the worst case value for components. It is always better to use pessimistic values in a reliability evaluation.

Power electronics often contribute most of all electronic components to the total MTTFd.

If no reliability data can be found for an electronic component or module use 10 years (e.g. standard industrial PLCs).

5.1.4 Estimation of MTTFd for electromechanical, pneumatic or hydraulic components

The procedure of estimating the MTTFd for electromechanical components (relays, contactors, pushbuttons, levers limit switches, guard interlocks etc), pneumatic components and hydraulic components is clearly described in Annex C in the standard.

B_{10d} is the number of operations a set of electromechanical or pneumatic components can perform until 10% of the set of components failed dangerously. This value is derived in a B_{10}-test and is to be acquired from the component manufacturer.

The B_{10d}-value is used to estimate the MTTFd for the components. However, B_{10d}-values are not considered applicable for hydraulic components. The reason for this is not motivated in the standard.

In order to be able to use Table C.1 in the standard which prescribes B_{10d}-values for electromechanical, pneumatic components and a MTTFd value for hydraulic components the requirements in Annex C.2 and C.3 shall be documented by the component manufacturer, e.g. in the datasheet. Otherwise the manufacturer shall deliver the B_{10d} value or the MTTFd value.

With a B_{10d} value available, the following formula may be used for deriving the MTTFd-value:

$$MTTFd = \frac{B_{10d}}{0{,}1 \times n_{op}}$$

Where n_{op} is the mean number of annual operations for the component. E.g. for a relay is one relay activation and the sub-sequent relay de-activation two operations. Equation C.2 in the standard suggests how n_{op} can be derived. However, to be able to show the rationale behind the estimation of n_{op} is more important than strictly applying Equation C.2.

For some components it is difficult for the component manufacturer to provide a B_{10d} value because it is application dependent which failures that actually are dangerous. In this case the manufacturer only provides a B_{10}-value. The following pessimistic assumption is in this case feasible (see Annex C.4.2, note 3 in the standard)):
$B_{10d} = 2 \times B_{10}$ (assuming that 50% of the components failure modes leads to dangerous failure effects)
In cases where the component manufacturer cannot provide a B10-value for the component, a pessimistic assumption that B10 equals the components specified electrical life as stated in the datasheet is permissible.

Because the MTTFd for electromechanical or pneumatic components depends on the application of the component it is common that these type of components has a large impact on the total SRP/CS MTTFd value.

Consider the following example using a contactor relay with maximum load (e.g. main motor contactor) which gives a B_{10d} of 400000 according to Table C.1in the standard.

n_{op} (mean relay contactor operations)	Relay contactor MTTFd [years]
1/year	4 million
1/month	333 thousand
1/week	77 thousand
1/day	10 thousand
1/hour	457
1/minute	8

5.1.5 Estimation of MTTFd for individual SRP/CS

When each safety related component is identified together with the SRP/CS structure every component is gathered in a spreadsheet (e.g. Excel or similar) and are grouped to their respective Input-block, Logic-block or Output block.

The designated architectures are in fact simplified reliability models based on a concept called channels. A channel is defined so that in all components within the channel there are failure modes which can cause the loss of the safety function. Each series of Input-Logic-Output is a channel and thus relates to the structures according to the following table:

Structure	Reliability model configuration
Category B	Single channel
Category 1	Single channel
Category 2	Single channel
Category 3	Dual channel
Category 4	Dual channel

According to the simplified method in the standard, Annex D the MTTFd of each channel is determined by the following formula:

$$\frac{1}{MTTF_{d,channel}} = \sum_{i=1}^{K} \frac{n_i}{MTTF_{d,i}}$$

Where:
i is the component type
K is the number of different component types within the channel
n_i is the number of components of type *i* within the channel
$MTTF_{d,i}$ is the $MTTF_d$ value for the particular component type *i*

No hardware solely used for implement diagnostics shall be part of the SRP/CS estimated MTTFd

5.1.5.1 Example of estimating the MTTFd for a SRP/CS

Consider the following hypothetical SRP/CS:

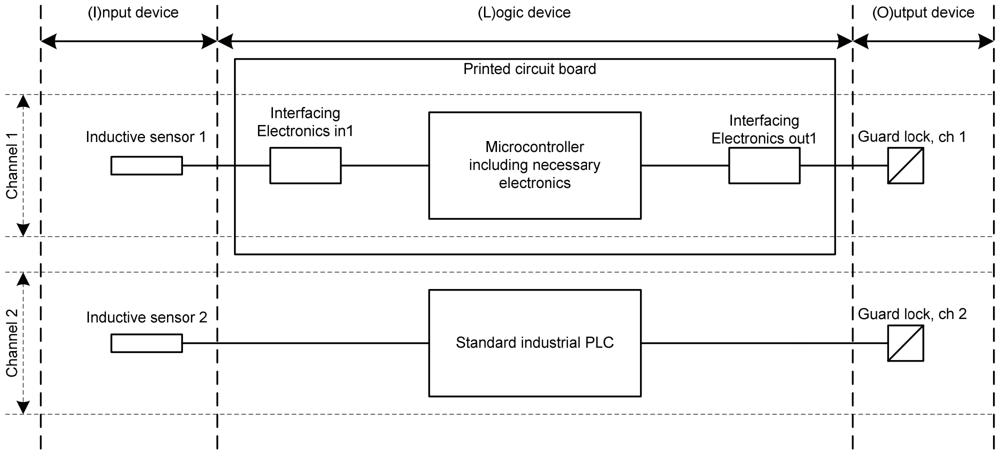


Figure 12 Fictive SRP/CS

This system is a fictive application specific SRP/CS. The safety function is a hatchet (guard) which shall remain physically locked with two hypothetical plungers preventing access to hazardous movement while a motor shaft rotates. The locking devices can only open the plungers with electromagnets controlled by the contactors. Power loss to the electromagnets causes mechanical locking of the hatchet by the plungers.

The SRC/PS shall fulfill PL_r = d.

Previously, the hardware has been analyzed (FMEA) and the structure category 3 was identified. The hardware was illustrated as channels excluding any diagnostics, i.e. no feedback signals, bus-communication between Microcontroller 1 and PLC, watchdogs etc. are included. The two channels were also found to be not identical.

The estimation of the MTTFd was performed using the following two tables.

Note that some of the values in these tables are fictive and not intended for professional use.

Table A: MTTFd for Channel 1

Device	Block	Component	Source of MTTFd	Number of components $[n_i]$	$MTTF_d$ [years]	$n_i/MTTF_{d,i}$
Input	Sensor	B1, Inductive sensor 1, JXZ0K65J7	Datasheet provides λ_D	1	700	0.001429
Logic	Interfacing electronics in1	Suppressor	Table C	1	3196	0.000313
		Resistor, Metal film	Table C	3	114 155	0.000021
		Capacitor, Ceramic	Table C	2	4566	0.000438
		Inductor, Low freq.	Table C	1	4566	0.000219
	Micrcontroller 1 (Large)	IC1	Datasheet	1	1114	0.000298
	Interfacing electronic out1	Suppressor	Table C	1	3196	0.000313
		Resistor, Metal film	Table C	4	114 155	0.000035
		Capacitor, Ceramic	Table C	2	4566	0.000438
		MOS, power	Table C	1	228	0.004386
Output	Actuator	Contactor, NO	B_{10d} = 400 000, n_{op} = 24*365	1	457	0.002188
1/MTTFd Channel 1 = Add all calculated $n_i/MTTF_{d,i}$ in column 7 =						0.010677
Resulting MTTFd for Channel 1(inverse of the result of the previous row)					**94**	

Table B: MTTFd for Channel 2

Device	Block	Component	Source of MTTFd	Number of components $[n_i]$	$MTTF_d$ [years]	$n_i/MTTF_{d,i}$
Input	Sensor	B1, Inductive sensor 1, Jcomponent data	Datasheet provides λ_D	1	700	0.001429
Logic	N/a	PLC	Not available	1	10	0.1
Output	Actuator	Contactor, NO	B_{10d} = 400 000, n_{op} = 24*365	1	457	0.002188
1/MTTFd Channel 2 = Add all calculated $n_i/MTTF_{d,i}$ in column 7 =						0.103617
Resulting MTTFd for Channel 2(inverse the result of the previous row) =					**9**	

Clause 4.5.2 in the standard requires that the MTTFd for each channel is considered individually, if there are different MTTFd for two channels the lower shall be selected. In this example:
MTTFd Channel 1 = 94 years
MTTFd Channel 2 = 9 years

Means that MTTFd SRP/CS total = 9 years, and thus “low” according to Table 5 in the standard. According to Figure 5 it is only possible to reach PL = c for a category 3 structure if MTTFd = low which contradicts the previous PL_r = d.

However, the standard provides a technique in order to resolve this problem by allowing the use of the following formula:

$$MTTF_{d,eqv} = \frac{2}{3}[MTTF_{d,ch1} + MTTF_{d,ch2} - \frac{1}{\frac{1}{MTTF_{d,ch1}} + \frac{1}{MTTF_{d,ch2}}}]$$

Which in this example would provide:

$$MTTF_{d,eqv} = \frac{2}{3}[94 + 9 - \frac{1}{\frac{1}{94} + \frac{1}{9}}] = 63 \text{ years}$$

This SRP/CS MTTFd value is within the interval for “high” MTTFd and thus is sufficient for PL = d according to Table 5 in the standard.

6 Diagnostic coverage (DC_{avg})

Aim:
The aim of this chapter is to discuss the concept and meaning of diagnostic coverage (DC) and to enlighten some techniques which may be applied in order to estimate the DC for a function or a module included in a SRP/CS.

Recalling Chapter 5.1.1 in this report, the failure rate for a component can be subdivided into different fractions depending on the components different failure mode effects on the control system (λ_D and λ_S). If automatic self-checking and error detecting mechanisms are included in the control system and which detects certain dangerous failures a third fraction can be derived from the FMEA called λ_{DD} which means dangerous detected failure rate.

What is diagnostic coverage?
The formal definition of diagnostic coverage is:

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_D} [\%]$$

Where:
$\sum \lambda_D$ = The fraction of the SRP/CS total failure rate which leads to a dangerous system failure, e.g. the loss of the safety function (*dangerous failure rate*); and
$\sum \lambda_{DD}$ = The fraction of the SRP/CS total dangerous failure rate which is detected (**AND** handled) by automatic and self monitoring mechanisms that are implemented in the SRP/CS or by other systems external to the SRP/CS.

Safety-related faults may also be revealed (detected) by manual tests or inspections. However, the coverage of such procedures **does not** contribute to the diagnostic coverage.

When a fault is detected?
When a fault is detected, the monitoring mechanisms shall handle the fault by initiate an appropriate action which is application dependent. For many applications within the machinery sector such an appropriate action is to initiate a so called safe-state (i.e. the safety-function is performed). The term safe-state implies that the control system removes the hazard instantly (e.g. by immediately stopping/preventing hazardous movement of a part of a machine by remove the power to a motor). For other machines or applications other actions may be more appropriate, such as issuing an alarm.
Unfortunately ISO 13849 does not define the term safe-state (at all) but refers to this term anyway at several locations. In IEC 61508:2010, Part 4, Clause 3.1.13 the term "safe-state" is defined as:

safe state
state of the EUC when safety is achieved

NOTE In going from a potentially hazardous condition to the final safe state, the EUC may have to go through a number of intermediate safe states. For some situations a safe state exists only so long as the EUC is continuously controlled. Such continuous control may be for a short or an indefinite period of time.
Note: EUC = Equipment Under Control (i.e. the machine)

With regard of this definition the following general conclusions of the term "safe-state" can be made:

- There is no pre-defined/standardized control system output state which shall be achieved in order to enter safe-state (e.g. all outputs de-energized)
- The safe-state can be entered by a controlled sequence
- The machine does not have to be stopped when the safe-state is entered

There are two important properties to consider regarding diagnostic means

The machine control system reaction of a failure

The machine control system reaction on a failure may be visualized in accordance to the following figure:

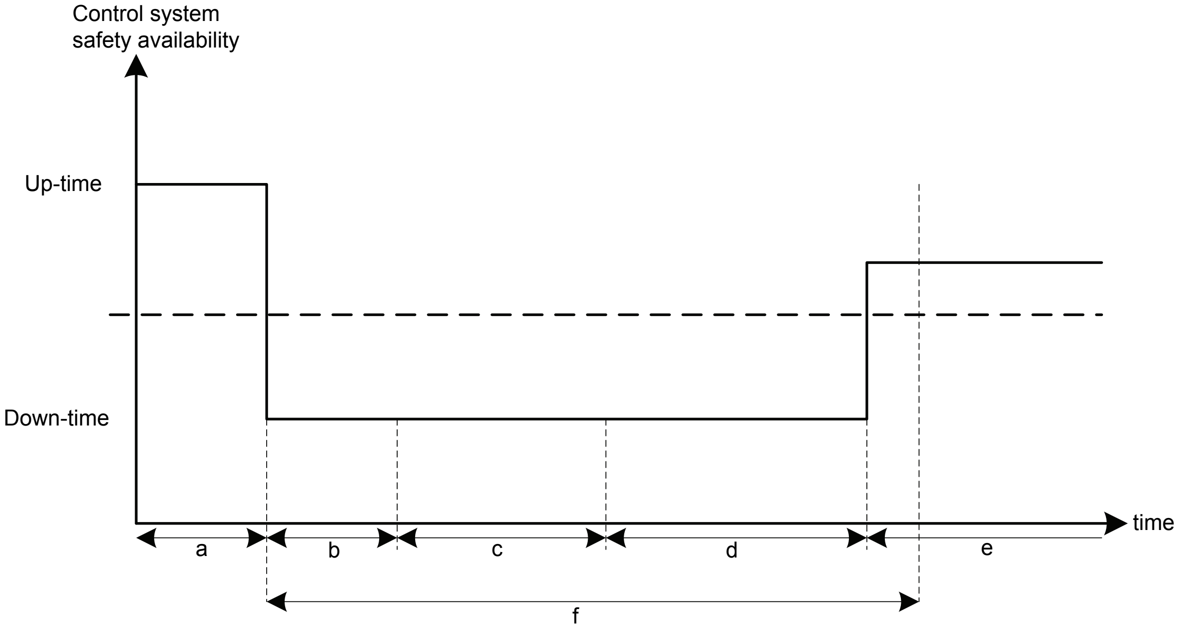


Figure 13 Machine behaviour when a fault occurs

Figure 9 is subdivided into the following time intervals
a – During this time interval the machine operates according to its specification (i.e. safe operation
b – A fault (e.g. random hardware fault) has occurred in the control system, the machine may now operate dangerously
c – The control system detects and registers the fault by internal diagnostic mechanisms and initiate a preventive action
d – During this time period the machine performs its preventive actions (e.g. applying brakes, remove power from drives)
e – During this time the machine is in its safe state
f – The time elapsed between a failure and the hazardous event without considering diagnostic mechanisms

If possible (b + c + d) shall be less than f.

The periodicity of conducting diagnostic tests

If a diagnostic test is not performed frequently enough, there is a probability that a failure causes a hazardous event between tests.

Requirements:
Table 6 in the standard specifies four levels of diagnostic coverage according to the following table:

Denotation	Range
None	DC < 60%
Low	60% ≤ DC < 90%
Medium	90% ≤ DC < 99%
High	99% ≤ DC

(see Annex E) the average diagnostic coverage for the whole SRP/CS be estimated using the following equation (when applying the simplified method):

$$DC_{avg} = \frac{\sum_{n=1}^{k} \frac{DC_n}{MTTF_{d,n}}}{\sum_{n=1}^{k} \frac{1}{MTTF_{d,n}}}$$

Guidance:
It is important to consider the robustness of the machine operation when designing diagnostic techniques in order to avoid unnecessary loss of production and/or to reduce the risk that the machine operator tries to tamper with safety functions.

One example where trimming of the diagnostic test technique is when applying cross monitoring of the feed-back signals from two redundant electromechanical components. Even if the components are identical they will have different response times (so called discrepancy times). Therefore the control system must tolerate a certain time deviation between the feedback signals. The length of the maximum allowed time deviation is to be determined in the hazard and risk analysis. A similar reasoning is applied when measuring analog values etc.

Examples of possible (non-exhaustive) interpretations of the implementation of some diagnostic techniques is presented in Appendix B in this report.

7 Common cause failure

In machinery applications where the need of a high degree of safety is needed a common structure of the control system is a redundant architecture. The redundant structure is efficient to control random failures occurring in only one of the redundant channels. But common cause failures (CCF) can affect both channels in a negative way. Examples of CCF are short circuits, extreme temperatures and electromagnetic interference.

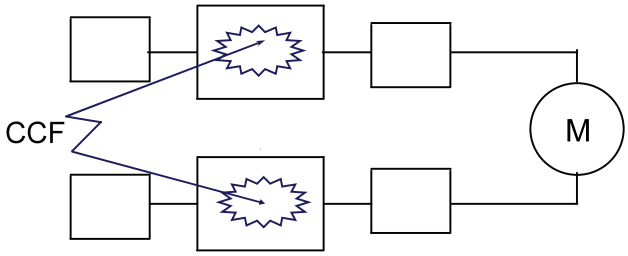


Figure 14 A single common cause failure affects two channels

In order to prevent that a common cause failure can affect safety the aim is to reduce the probability for common cause failures. During the design phase of a SRP/CS it is possible to implemented measures in order to reduce the probability for common cause failures.

The standard requires the performance level of the control system shall be determined with estimation of CCF as one important aspect. An assessment of CCF is necessary for every safety validation, but can be performed in different ways.

The standard has a procedure for estimating the CCF measures implemented for SRP/CS with a category 2, 3 or 4 structures. The procedure is presented by a score table F.1 in the standard. The proposed procedure is described in an informative part of the standard. Other procedures can be used to judge measures against CCF, but the proposed score table F.1 is commonly applied. The score table covers the following areas:

- Separation/ Segregation of signal cables and also creepage distances on printed-circuit boards
  The intention is to avoid short circuits between the redundant channels. It is usually very important when static input and output signals are used. The need for separation may be reconsidered when dynamic signals are used.
- Diversity in technologies, design or physical principles
  The intention is to reduce the probability of a fault affecting both channels. An example is different sensitivity to electromagnetic interference in different components, e.g. an electromechanical or an electronic sensor. Another example is when diversity in software is applied to reduce the risk of a programming mistakes affecting both channels.
- Design/application/experience
  The intention is to reduce the probability of an external factor affecting both channels at the same time. An example is when a high voltage transient bursts from inductive loads destroys electronic components in both channels.
- Failure mode and effect analysis covering CCF failures
  The intention is to identify critical components of the design and reduce the probability of a fault appearing in both channels.

- Competence/training in order to understand the causes and consequences of CCF
  Both design engineers and maintenance staff should be trained to understand the significance of reducing CCF.
- Suitable design with respect to environmental impact
  Environmental aspects may affect both channels at the same time. An example is that EMC performance of the design has been tested and approved. This will reduce the probability of a disturbance affecting both channels.

For each area above points are presented. In order to fulfill the requirements a score of minimum 65 points or better is needed. For each listed measure, only the full score or nothing can be clained. If a measure is only partly fulfilled, the score according to this measure is zero. The maximum score is 100 points. When performing the assessment, a motiviation for every judgment shall be noted.

Example of how measures against CCF can be estimated using the method proposed in the standard:

No	**Measure against CCF**	**Max score**	**Achieved score**
1	Separation / segregation	15	15
2	Diversity	20	20
3.1	Design: Protection against overvoltage, current, etc.	15	15
3.2	Design: Components are well tried	5	0
4	Assessment / analysis	5	5
5	Competence / training	5	0
6.1	Environmental: EMC	25	25
6.2	Environmental: Other influences	10	10
	Total	100	90

8 Software

Today many safety functions are depending on both correct functioning of the hardware and correct functioning of the software. Earlier, mainly non safety critical functions were implemented in software and safety critical functions were traditionally hard-wired. The introduction of fail safe PLCs made it possible to also realize safety critical functions by software.

It is of course an advantage to be able to realize both safety critical and non safety critical in the same fail safe PLC, but it is important to understand that safety is not automatically reached in this case and that you still as software developer has got the responsibility to develop a safe software. Situations that you must try to avoid is for instance that a logical fault in the software does not give an unexpected start of the machine.

The standard gives support to the software designer what to think about during the different steps of the software safety lifecycle to, as far as it is possible, minimize that faults are introduced.

8.1 General requirements

In the standard two different types of languages are defined

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

Chapter 3.1.34 in the standard

Limited variability languages are typically [6] languages that are used in fail safe PLC when developing the application software.

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

Chapter 3.1.35 in the standard

An example when full variability languages are used are when the manufacturers of fail safe PLCs are developing the embedded software running inside the fail safe PLC. Examples of FVL are for instance C and C++.

application software
software specific to the application, implemented by the machine manufacturer to meet the SRP/CS requirements

Chapter 3.1.36 in the standard

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

Chapter 3.1.37 in the standard

For the application software the abbreviation SRASW (safety-related application software) is used

For the embedded software the abbreviation SRESW (safety-related embedded software) is used.

The figures below describes the connection between SRESW and SRASW and that parameterization of both application SW and embedded SW can be performed by an external parameterization tool:

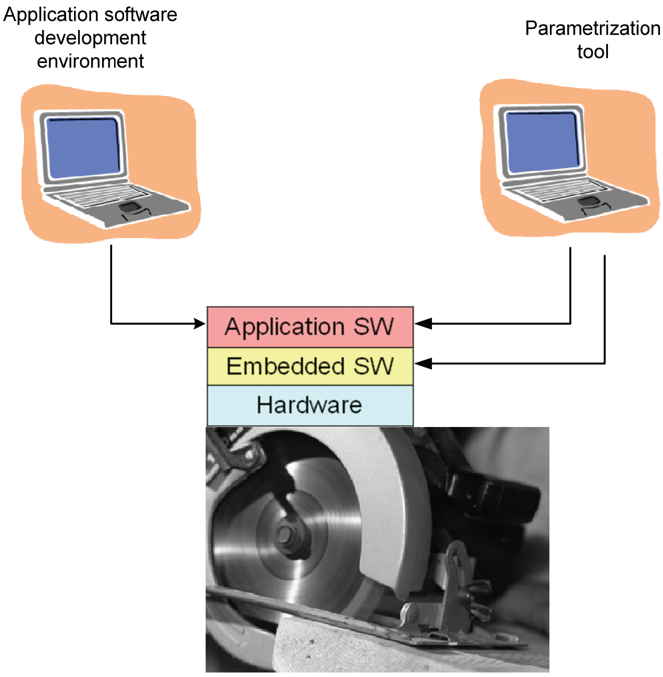
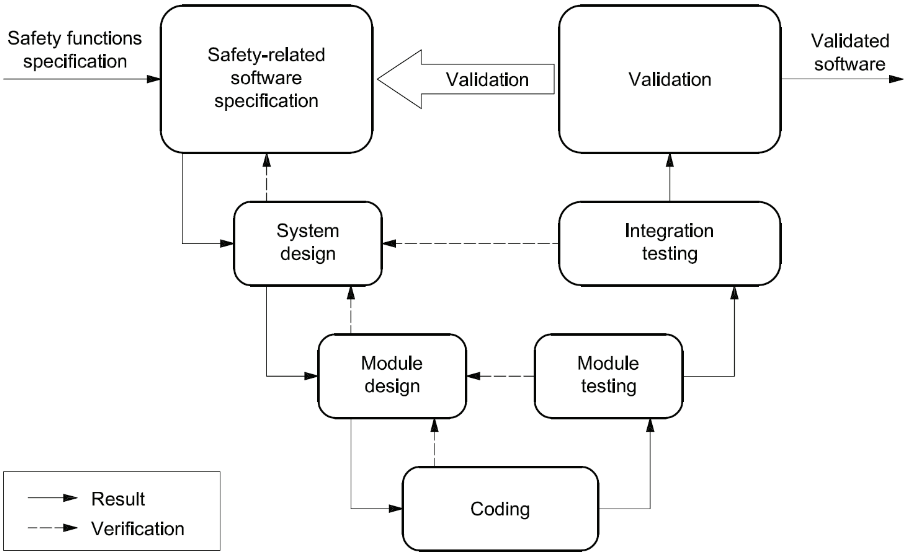


Figure 15 Relation between SRESW and SRASW

From the figure above, it is possible to see that the embedded software has a closer connection to the hardware than the application software.

The operating system in a fail-safe PLC is an example of an embedded software while writing code in [6] languages in a development environment from a manufacturer of a fail-safe PLC is an example of application software.

The aim with the V-model described in Figure 6 (Figure 16 on the next page) in the standard is to describe how the software shall be developed from receiving a safety functions specification until the software is validated.



NOTE Annex J gives more detailed recommendations for lifecycle activities.

Figure 16 Simplified V model of software lifecycle

In the standard the overall requirements as defined in the V-model is summarized as:

> The main objective of the following requirements is to have readable, understandable, testable and maintainable software
>
> Chapter 4.6.1 in the standard

In Figure 6 in the standard also verification activities are included (dashed arrows). The aim of the verification is to check that each phase in the software safety life cycle has been performed correctly. An example of a verification activity is that a person, that has not been involved in the development of the safety-related software specification reviews this document to check that it is correct and fulfils the applicable requirements in the standard

> SRESW and SRASW written in FVL for components with **PLr = e** shall comply with IEC 61508-3:1998, Clause 7, appropriate for **SIL 3**.
>
> Chapter 4.6.2 in the standard

> If SRASW is written in FVL, the requirements for SRESW shall apply and **PL a to e** is achievable.
>
> Chapter 4.6.3 in the standard

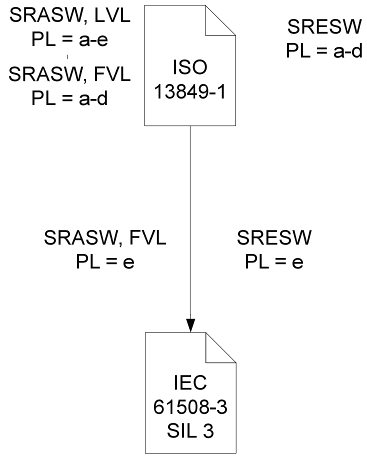


Figure 17 Relations between ISO 13849-1 and IEC 61508-3 for software

The standard also points out that it is important to document the result from each software safety life cycle phase and that the documentation shall be complete, available, readable and understandable. The reason for this is that it shall be possible to go back after a project is finalized and check how is step in the software safety life cycle is performed.

The following additional measures for SRESW for components with PLr c-d are described in the standard:

- *project management and quality management system comparable to, e.g. IEC 61508 or ISO 9001*
- *configuration management to identify all configuration items and documents related to a SRESW release*

For SRASW, written in LVL, for components with PLr from c to e, the following additional measures with increasing efficiency (lower for PLr of c, medium for PLr of d, higher for PLr of e) are required or recommended:

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

8.2 Safety-related software specification

The first phase in the V-model is to develop a safety-related software specification. In this phase it is important to read through the safety requirements specification for each safety function and check which of these requirements that influence or need to be further detailed in the safety-related software specification. Below follows a number of aspects that needs to be considered in the safety-related software specification:

- safety functions with required PL and associated operating modes
- performance criteria, e.g. reaction times

- real time properties
- hardware architecture with external signal interfaces detection and control of external failure
- detection and management of faults in sensors, logic units, actuators, and in the software itself (self-diagnosis)
- operating modes

When the safety-related software specification is developed it shall be verified. One example of verification activity in this case can be that a person that has not been involved in the development of the safety-related software specification goes through this document and check it for correctness.

Documentation:

Safety-related software specification.
Safety-related software validation plan

8.3 System- and module design

When the safety-related software specification is ready, it is possible to go on with the system- and module design. The aim with this phase is to give a high level description of how the software will function. When possible, it is preferrable to divide the system into a number of different modules. One reason for this is that the risk for introducing faults when coding will be reduced and it will also be possible to test each module separately.

During this phase, it is also important to define how each module shall be tested. This information is described in the System- and module test plan.

For SRASW, written in LVL, for components with PLr from c to e, the following additional measures with increasing efficiency (lower for PLr of c, medium for PLr of d, higher for PLr of e) are required or recommended:

- *semi-formal methods to describe data and control flow, e.g. state diagram or program flow chart*
- *modular and structured programming predominantly realized by function blocks deriving from safety related validated function block libraries*
- *function blocks of limited size of coding*
- *code execution inside function block which should have one entry and one exit point*
- *architecture model of three stages, Inputs ⇒ Processing ⇒ Outputs*
- *assignment of a safety output at only one program location*
- *use of techniques for detection of external failure and for defensive programming within input, processing and output blocks which lead to safe state*

Documentation:

System- and module design specification
System- and module test plan

8.4 Coding

When the system- and module design is ready the next step is to start writing the detailed code for each module in the system.

The following additional measures for SRESW for components with PLr c-d are described in the standard:

- *use of suitable programming languages and computer-based tools with confidence from use*
- *modular and structured programming, separation in non-safety-related software, limited module sizes with fully defined interfaces, use of design and coding standards*

For SRASW, written in LVL, for components with PLr from c to e, the following additional measures with increasing efficiency (lower for PLr of c, medium for PLr of d, higher for PLr of e) are required or recommended:

Selection of tools, libraries, languages:

- *Suitable tools with confidence from use: for* ***PL = e*** *achieved with one component and its tool, the tool shall comply with the appropriate safety standard; if two diverse components with diverse tools are used, confidence from use may be sufficient. Technical features which detect conditions that could cause systematic error shall be used. Checks should mainly be carried out during compile time and not only at runtime. Tools should enforce language subsets and coding guidelines or at least supervise or guide the developer using them.*
- *Validated function block (FB) libraries should be used — either safety-related FB libraries provided by the tool manufacturer (highly recommended for* ***PL = e****) or validated application specific FB libraries and in conformity with this part of ISO 13849.*
- *A justified LVL-subset suitable for a modular approach should be used, e.g. accepted subset of IEC 61131-3 languages. Graphical languages (e.g. function block diagram, ladder diagram) are highly recommended.*

Where SRASW and non-SRASW are combined in one component:

- *SRASW and non-SRASW shall be coded in different function blocks with well-defined data links*
- *there shall be no logical combination of non-safety-related and safety-related data which could lead to downgrading of the integrity of safety-related signals*

Software implementation/coding:

- *code shall be readable, understandable and testable*
- *justified or accepted coding guidelines shall be used*
- *data integrity and plausibility checks (e.g. range checks) available on application layer (defensive programming) should be used*
- *code should be tested by simulation*
- *verification should be by control and data flow analysis for* ***PL = d or e****.*

Documentation:

- *code documentation within source text shall contain module headers with legal entity, functional and I/O description, version and version of used library function blocks, and sufficient comments of networks/statement and declaration lines.*

8.5 Module- and integration testing

The aim of the module test is to check that each module works as specified. The tests will be based on information in the System- and module test plan. After each module is tested, it is also important to check that the system is working as specified when integration the hardware and software.

Documentation:

Module test report
Integration test report

8.6 Software validation

The purpose of the software validation is to check that the software fulfills the requirements specified in the safety-related software validation plan. It is important to follow this safety-related software validation plan. The results of validation shall be documented and action plans on detected errors are specified.

Testing shall be the main validation method.

It is preferable if the validation is carried out by persons that are independent of design (to an appropriate level)

In some situations it can be more efficient to only have one validation that covers both hardware and software, instead of having two different validation activities (one for hardware and one for software)

The following measures for SRESW for components with PLr a-d are described in the standard:

- *software safety lifecycle with verification and validation activities*
- *where using software-based measures for control of random hardware failures, verification of correct implementation*
- *functional testing, e.g. black box testing*

The following additional measures for SRESW for components with PLr c-d are described in the standard:

- *coding verification by walk-through/review with control flow analysis*
- *extended functional testing, e.g. grey box testing, performance testing or simulation*

The following measures for SRASW written in LVL for components with PLr a-e are described in the standard:

- *functional testing*

For SRASW, written in LVL, for components with PLr from c to e, the following additional measures with increasing efficiency (lower for PLr of c, medium for PLr of d, higher for PLr of e) are required or recommended:

- *The safety-related software specification shall be reviewed, made available to every person involved in the lifecycle*

Testing:

- *the appropriate validation method is black-box testing of functional behaviour and performance criteria (e.g. timing performance);*
- *for **PL = d or e**, test case execution from boundary value analysis is recommended;*
- *test planning is recommended and should include test cases with completion criteria and required tools;*
- *I/O testing shall ensure that safety-related signals are correctly used within SRASW.*

Verification

- *using review, inspection, walkthrough or other appropriate activities. Verification is only necessary for application-specific code, and not for validated library functions.*

Documentation:

Software validation report

8.7 Software modifications

It is important to be careful when performing modification in safety-related software. The standard says that appropriate software safety lifecycle activities shall be performed. This means that before you change the code it is important to investigate how this change will influence the earlier work performed and whether certain safety life cycle phases needs to be updated.

The following additional measures for SRESW for components with PLr c-d are described in the standard:

- *impact analysis and appropriate software safety lifecycle activities after modifications*

For SRASW, written in LVL, for components with PLr from c to e, the following additional measures with increasing efficiency (lower for PLr of c, medium for PLr of d, higher for PLr of e) are required or recommended:

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

Documentation:

Impact analysis

8.8 Parameterization

In the standard much focus is placed on software-based parameterization. The reason for this is that software-based parameterization can be seen as an untyped programming language that can influence the safety of the machinery.

Following requirement can be found in Chapter 4.6.4 in the standard:

Software-based parameterization of safety-related parameters shall be considered as a safety-related aspect of SRP/CS design to be described in the software safety requirements specification.

In Chapter 4.6.4 in the standard it is possible to find more detailed information about which requirements that are placed on parameterization tools and different alternative ways to fulfill these requirements.

9 Achieved PL

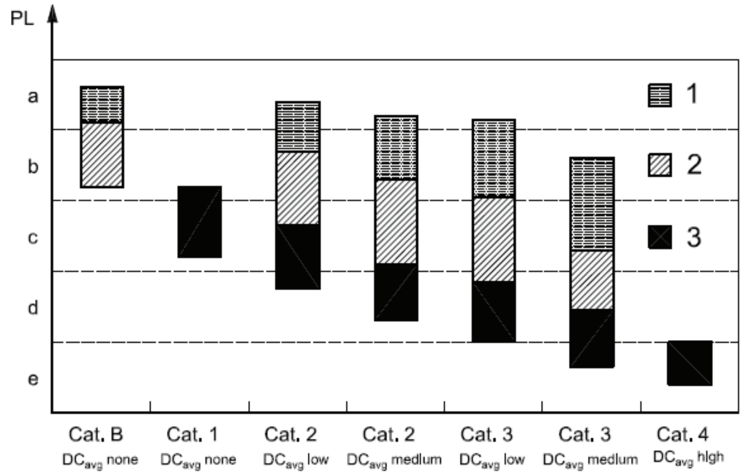
The standard describes a number of different methods of determining the PL for the identified safety functions.

The following methods will be described in this report:

- Apply Figure 5 in the standard in combination with Annex K in the standard
- Apply Table 7 in the standard
- Apply Table 11 in the standard

9.1 Apply Figure 5 in combination with Annex K

Below Figure 5 from the standard describes how a PL can be decided based on the category (for the SRP/CS), MTTFd (for each channel in the SRP/CS), DCavg (totally for the SRP/CS)



Key

PL performance level

1 $MTTF_d$ of each channel = low

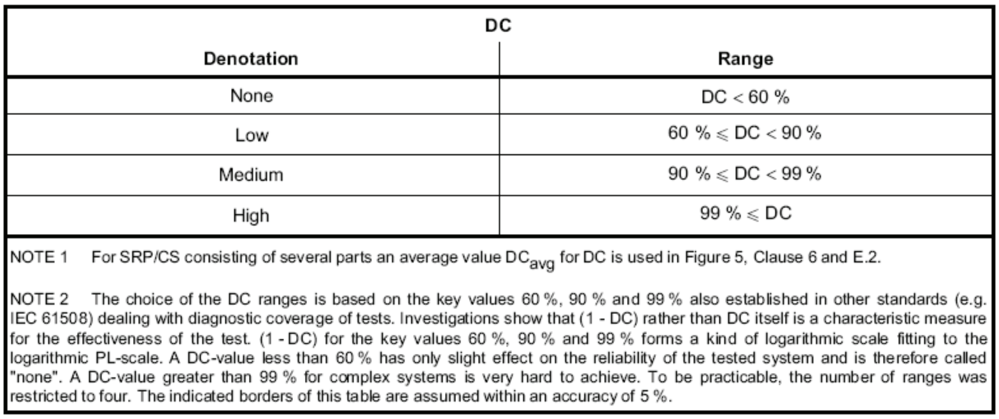
2 $MTTF_d$ of each channel = medium

3 $MTTF_d$ of each channel = high

Figure 18 Relationships between categories, DC_{avg}, $MTTF_d$ of each channel and PL

To be able to use this method, the architecture of the SRP/CS must be in accordance with a designated architecture (category). The next step after the category is decided is to decide which diagnostic coverage that is reached for the SRP/CS. Table 6 from the standard has defined four different levels

Table 6 — Diagnostic coverage (DC)



DC	
Denotation	Range
None	DC < 60 %
Low	60 % ⩽ DC < 90 %
Medium	90 % ⩽ DC < 99 %
High	99 % ⩽ DC

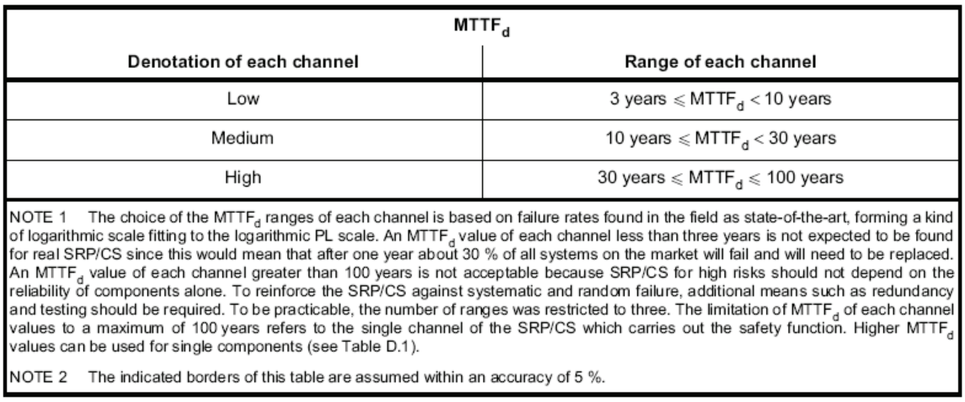
NOTE 1 For SRP/CS consisting of several parts an average value DC_{avg} for DC is used in Figure 5, Clause 6 and E.2.

NOTE 2 The choice of the DC ranges is based on the key values 60 %, 90 % and 99 % also established in other standards (e.g. IEC 61508) dealing with diagnostic coverage of tests. Investigations show that (1 - DC) rather than DC itself is a characteristic measure for the effectiveness of the test. (1 - DC) for the key values 60 %, 90 % and 99 % forms a kind of logarithmic scale fitting to the logarithmic PL-scale. A DC-value less than 60 % has only slight effect on the reliability of the tested system and is therefore called "none". A DC-value greater than 99 % for complex systems is very hard to achieve. To be practicable, the number of ranges was restricted to four. The indicated borders of this table are assumed within an accuracy of 5 %.

More information about diagnostic coverage can be found in Chapter 6 in this report.

The last step after the category and diagnostic coverage is chosen is to decide the MTTFd reached for the SRP/CS. Below Table 5 from the standard has defined three different levels.

Table 5 — Mean time to dangerous failure of each channel ($MTTF_d$)



$MTTF_d$	
Denotation of each channel	Range of each channel
Low	3 years ⩽ $MTTF_d$ < 10 years
Medium	10 years ⩽ $MTTF_d$ < 30 years
High	30 years ⩽ $MTTF_d$ ⩽ 100 years

NOTE 1 The choice of the $MTTF_d$ ranges of each channel is based on failure rates found in the field as state-of-the-art, forming a kind of logarithmic scale fitting to the logarithmic PL scale. An $MTTF_d$ value of each channel less than three years is not expected to be found for real SRP/CS since this would mean that after one year about 30 % of all systems on the market will fail and will need to be replaced. An $MTTF_d$ value of each channel greater than 100 years is not acceptable because SRP/CS for high risks should not depend on the reliability of components alone. To reinforce the SRP/CS against systematic and random failure, additional means such as redundancy and testing should be required. To be practicable, the number of ranges was restricted to three. The limitation of $MTTF_d$ of each channel values to a maximum of 100 years refers to the single channel of the SRP/CS which carries out the safety function. Higher $MTTF_d$ values can be used for single components (see Table D.1).

NOTE 2 The indicated borders of this table are assumed within an accuracy of 5 %.

When applying Figure 5 in the standard it is important to be careful when the MTTFd level is chosen (MTTFd=Low, MTTFd=Medium or MTTFd=High) covers more than one designated architecture (category) and in this case it will be necessary to go into Annex K and check exactly at which value of MTTFd the PL switches from one level to another.

9.2 Apply Table 7

Table 7 in the standard is similar to Figure 5 in the standard with the difference that it is more conservative, in effect in those cases where the chosen MTTFd value (MTTFd=Low, MTTFd=Medium, MTTFd=High) in Figure 5 covered two PL levels only the lowest PL can be reached when applying Table 7.

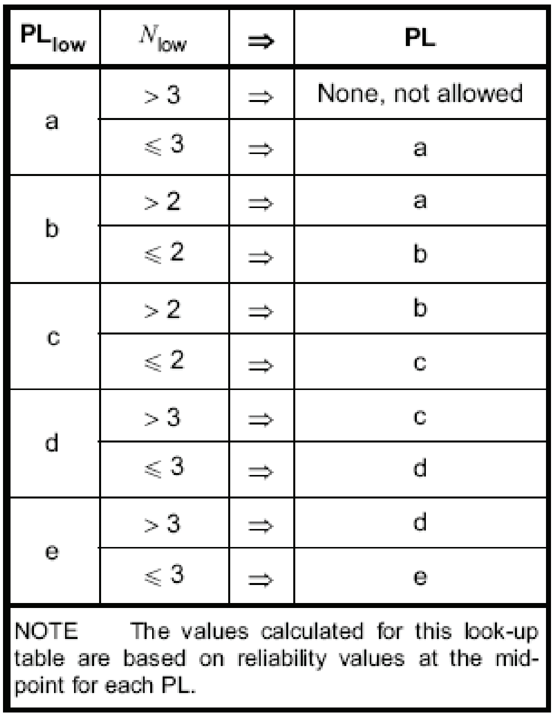
This gives a conservative approach, but on the other hand it is an very easy method where it will not be necessary to go into Annex K and check the exact limit between different PL levels.

9.3 Apply Table 11

In some situations it is not possible to use Figure 5 or Table 7 in the standard. This is for instance the situation when you shall combine different SRP/CS with different designated architectures (categories) to a safety function.

Below Table 11 in the standard describes how to reach a PL for the safety function.

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



PL_{low}	N_{low}	⇒	PL
a	> 3	⇒	None, not allowed
	⩽ 3	⇒	a
b	> 2	⇒	a
	⩽ 2	⇒	b
c	> 2	⇒	b
	⩽ 2	⇒	c
d	> 3	⇒	c
	⩽ 3	⇒	d
e	> 3	⇒	d
	⩽ 3	⇒	e

NOTE The values calculated for this look-up table are based on reliability values at the mid-point for each PL.

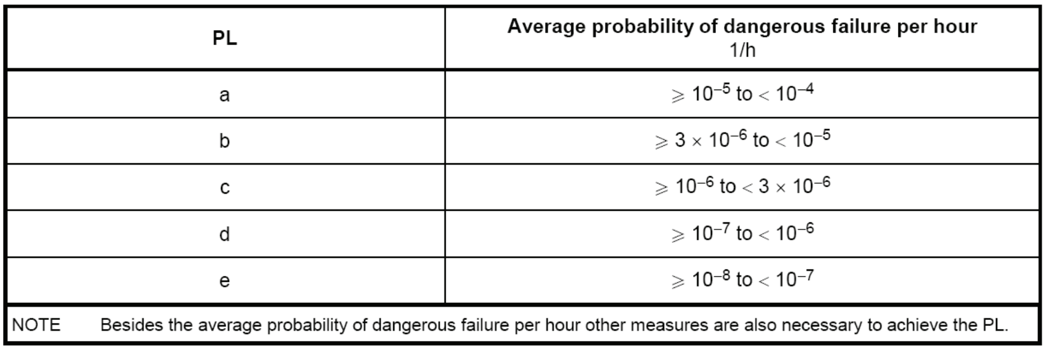
It is important to point out that Table 11 in the standard can only be used for SRP/CS that are connected in serial (in effect no redundant architecture). When using Table 11 in the standard the first step is to identify how many (called N_{low}) SRP/CS that has got the lowest PL, called PL_{low}.

As an example if PL_{low} is c and N_{low} is less than or equal to two than the PL reached for the complete safety function will be PL=c. If N_{low} instead had been higher than two the PL reached for the complete safety functions would have been decreased to PL=b.

When using Table 11 in the standard it is important to consider the interfaces between these different SRP/CS and check in the safety manuals for each SRP/CS how it shall be connected to other SRP/CS.

Table 11 in the standard is conservative and one alternative way is to summarize the PFH_D value for each SRP/CS and then use below Table 3 from the standard to check which PL the summarized PFH_D corresponds to:

Table 3 — Performance levels (PL)



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

NOTE Besides the average probability of dangerous failure per hour other measures are also necessary to achieve the PL.

10 Conclusions

EN ISO 13849-1:2008 gives a good support both for companies developing control systems and for machine builders.

EN ISO 13849-1:2008 does only briefly mention management issues and thus this report has thoroughly described the meaning of management of functional safety. The description was based on Figure 3 in the standard, which gives an overview of the complete safety life cycle, from risk assessment to modification of safety systems.

An advantage with EN ISO 13849-1:2008 compared to EN 954-1:1996 is that it is more flexible concerning how to use categories. In EN 954-1:1996 a direct connection existed between the risk assessment and which category that was required. In EN ISO 13849-1:2008 the result of the risk assessment is instead that a certain PL_r is required for each safety function (and not directly a certain category) and to reach this PL_r it is possible to combine categories, $MTTF_D$ and DC_{avg} in different ways. What this means is that in certain cases a lower category can be compensated by using reliable components (high $MTTF_D$) and implement different kinds of diagnostic techniques (high DC_{avg}).

This report gives a detailed description of how to interpret the different categories (designated architectures) described in EN ISO 13849-1:2008 together with a practical example.

Also the meaning of $MTTF_D$ is described both the background theory and also how it can be applied.

Another central part of EN ISO 13849-1:2008 is diagnostic coverage. This report describes the meaning of diagnostic coverage and also includes a number of different examples on how to interpret the diagnostic techniques described in Table E.1 in EN ISO 13849-1:2008.

The report also describes the difference between systematic failures and common cause failures.

The description of the software in the report is made outgoing from the different phases in the V-model.

Finally the report describes a number of different methods to determine the overall PL for the safety functions.

Appendix A Safety requirements specification – machinery

This appendix presents a template for the safety requirements specification for safety functions intended for machinery applications.

A safety function has the following definition: a function of the machine whose failure can result in an immediate increase of the risk(s). Parts of machinery control systems that are assigned to provide safety functions are called safety-related parts of control systems (SRP/CS).

The standard does not give support or requirements on the content of a safety requirements specification for the design of safety functions. Requirements are instead focused on the software safety requirements, the specification of safety functions and details of safety functions.

All relevant information for the required functionality of the safety functions shall be described and it is important that requirements are described in a way to avoid misunderstandings. The safety requirements specification is an important document during verification and validation activities.

In some cases, the information regarding the machinery may not be possible to get before the design process of the machine is started. In this case the safety requirements specification needs to be updated during the design process.

The result of the risk analysis for the machinery is the base for the requirements as well as the intended use for the machinery and expected environmental aspects for the machinery. The following is an example of what is needed:

- Functional description of the machinery
- The work modes of the machinery
- The identified safety functions
- Functional description of the safety functions
- Cycle time of the machinery
- Response time of the machinery
- Environmental conditions
- Interactions between human and the machine

Inspection of the safety requirements specification is needed in order to avoid incompleteness and contradictions in the specifications. The examination should (if possible) be carried out by a team that was not involved in the creation of the specification. The required level of independence needs to be determined.

Template for the Safety requirements specification

Specify responsible person for the Safety requirements specification. The work can be split on several persons with suitable competence e.g. hardware, mechanics, software.

<table>
<tr><th colspan="2">Responsible</th></tr>
<tr><td colspan="2">Main responsible: *Name/Company/E-mail/Telephone*</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>Responsible</td><td>Competence area</td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
</table>

General description

<table>
<tr><th colspan="2">General description of the machinery</th></tr>
<tr><td>Name of the machine</td><td>Manufacturer</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">Identification of the machine *e.g. type/ serial no.*</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2">Functional description of the machine</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>Working modes *(e.g. automatic. manual, setting, service, cleaning)*</td><td>Priority of working modes *(if any)*</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">Interactions between the human and the machine *(e.g. setting, cleaning, maintenance)*</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>Cycle time</td><td>Response time</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">Environmental conditions *(temperature, water, dust, vibration)*</td></tr>
<tr><td colspan="2"></td></tr>
</table>

Supporting documents

Describe the documents that have been used as support.

Machinery documentation	
Name of the risk analysis.	Identification *(e.g. version or date)*
Other supporting documents	Identification *(e.g. version or date)*

Identified safety functions

Summarize the identified safety functions and verify that they are safety related. This work needs knowledge of the function of the machine and the risks associated.

Identified safety functions	
Safety function	Safety critical (Yes/No)
1.	
2.	
3.	
4.	
5.	
6.	

The safety critical functions shall have a PL according to the requirements (the risk analysis or product standard).

Comments regarding the safety function	
Safety function	Comment

Description of the safety function

Describe each individual safety function by using the template below:

Description of the safety function	
Name of the safety function	
Hazard(s) associated	Performance Level required PL_r
	PL_r =
Type of safety function	*Example of safety functions:* • Safety related stop function initiated by a safety function • Emergency stop • Manual reset • Start/ restart • Control function • Muting • Hold to run • Activation function • Mode selector for control or operating modes • Start function • Prevention of unexpected start • Emergency rescue of draw in hazards • Isolating function or energy dissipation function
When shall the safety function be activated (normally all operating modes)	
Activating factor (the trigger)	Expected usage? *e.g. how often will the safety function be activated?*
Action when the safety function is activated	
Description of the safe state	
Fault behavior of the machine when a fault is detected:	
Affects the response time of the machine safety? Yes/No Maximum response time or stop time?	
Description of the interface to other machines or safety functions	

Action plan

Action plan for remaining activities:

Action plan				
Activity	Responsible	Finish date	Activity OK y/n?	Comment

Verification of the safety requirements specification

Specify the verification activities.

Verification activities				
Verification activity	Responsible	Finish date	Activity OK y/n?	Comment

Appendix B Examples of diagnostic techniques

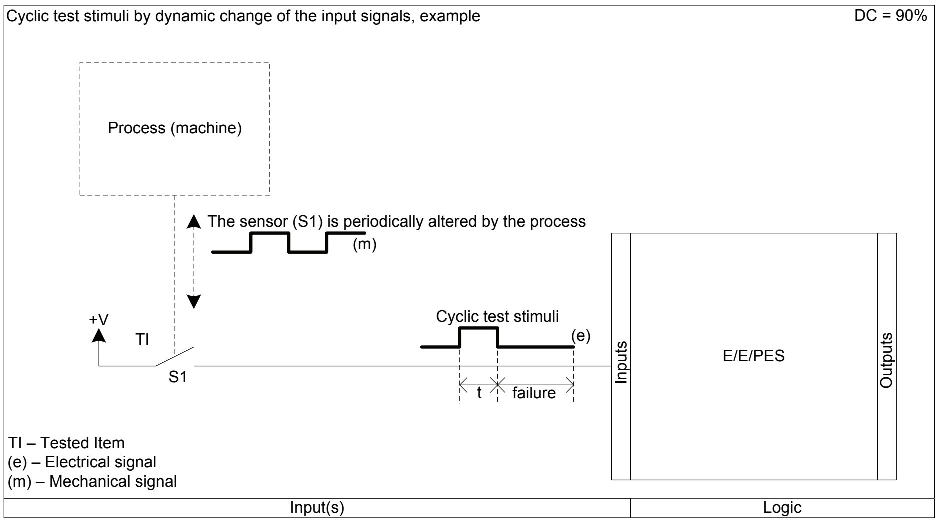


Figure 19 Cyclic test stimuli by dynamic change of the input signal

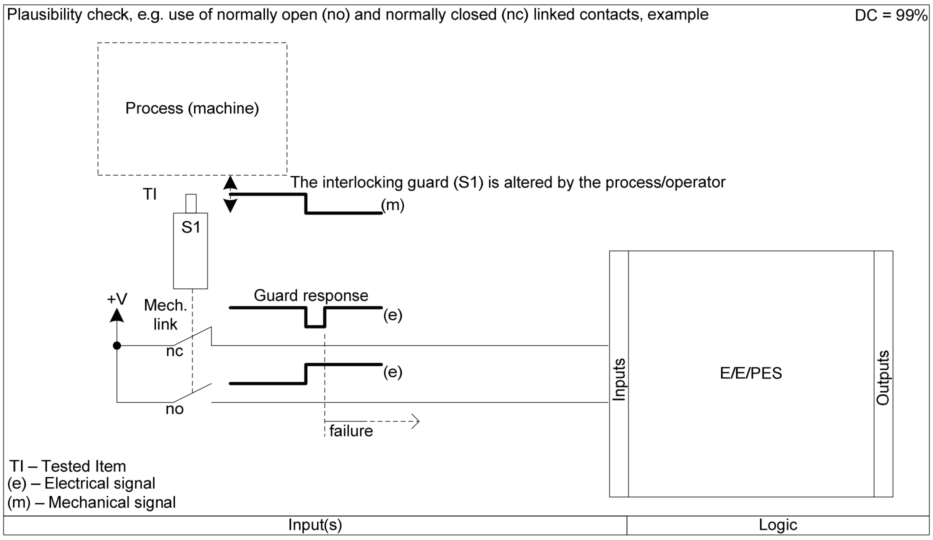


Figure 20 Plausibilty check

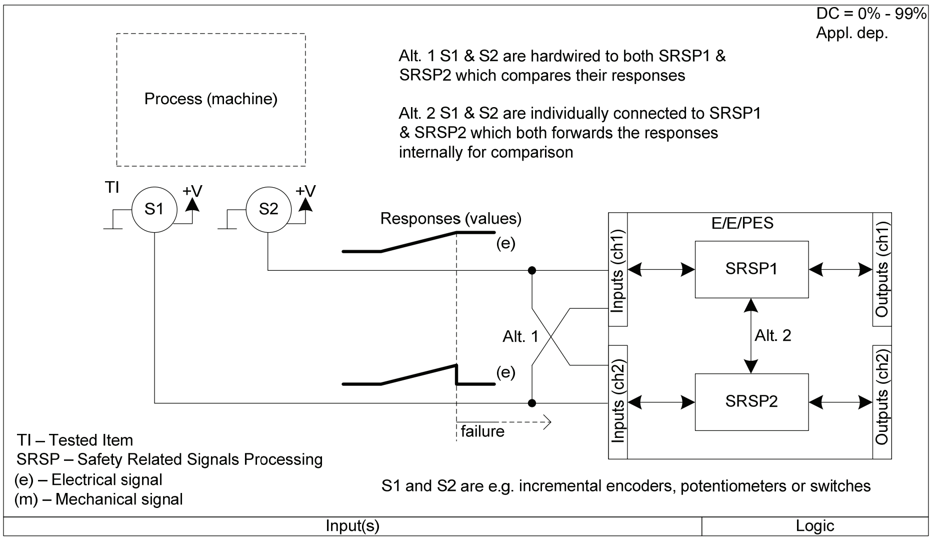

DC = 0% - 99%
Appl. dep.
Process (machine)
Alt. 1 S1 & S2 are hardwired to both SRSP1 & SRSP2 which compares their responses
Alt. 2 S1 & S2 are individually connected to SRSP1 & SRSP2 which both forwards the responses internally for comparison
TI
S1
+V
S2
+V
Responses (values)
(e)
(e)
Alt. 1
failure
E/E/PES
Inputs (ch1)
SRSP1
Outputs (ch1)
Alt. 2
Inputs (ch2)
SRSP2
Outputs (ch2)
TI – Tested Item
SRSP – Safety Related Signals Processing
(e) – Electrical signal
(m) – Mechanical signal
S1 and S2 are e.g. incremental encoders, potentiometers or switches
Input(s)
Logic

Figure 21 Cross monitoring of inputs without dynamic tests

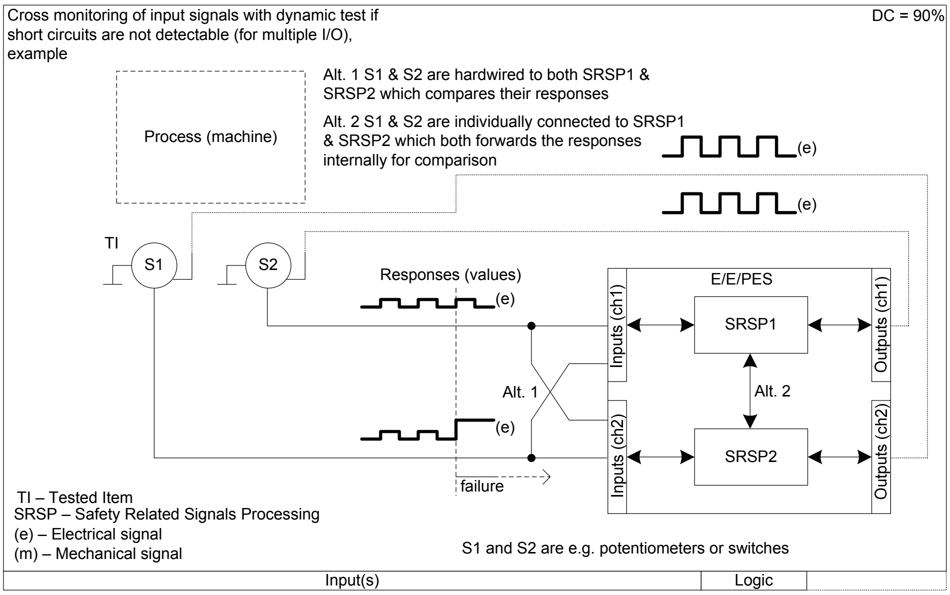

Cross monitoring of input signals with dynamic test if short circuits are not detectable (for multiple I/O), example
DC = 90%
Alt. 1 S1 & S2 are hardwired to both SRSP1 & SRSP2 which compares their responses
Alt. 2 S1 & S2 are individually connected to SRSP1 & SRSP2 which both forwards the responses internally for comparison
Process (machine)
(e)
(e)
TI
S1
S2
Responses (values)
(e)
(e)
E/E/PES
Inputs (ch1)
SRSP1
Outputs (ch1)
Alt. 1
Alt. 2
Inputs (ch2)
SRSP2
Outputs (ch2)
failure
TI – Tested Item
SRSP – Safety Related Signals Processing
(e) – Electrical signal
(m) – Mechanical signal
S1 and S2 are e.g. potentiometers or switches
Input(s)
Logic

Figure 22 Cross monitoring of input signals with dynamic test

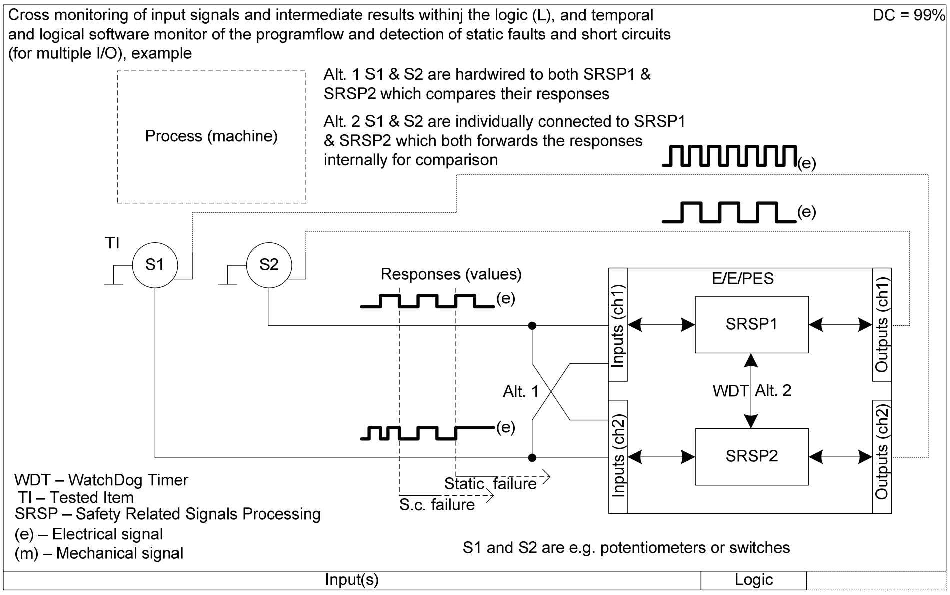

Cross monitoring of input signals and intermediate results withinj the logic (L), and temporal and logical software monitor of the programflow and detection of static faults and short circuits (for multiple I/O), example
DC = 99%
Alt. 1 S1 & S2 are hardwired to both SRSP1 & SRSP2 which compares their responses
Alt. 2 S1 & S2 are individually connected to SRSP1 & SRSP2 which both forwards the responses internally for comparison
Process (machine)
(e)
(e)
TI
S1
S2
Responses (values)
(e)
(e)
E/E/PES
Inputs (ch1)
SRSP1
Outputs (ch1)
Alt. 1
WDT
Alt. 2
Inputs (ch2)
SRSP2
Outputs (ch2)
Static failure
S.c. failure
WDT – WatchDog Timer
TI – Tested Item
SRSP – Safety Related Signals Processing
(e) – Electrical signal
(m) – Mechanical signal
S1 and S2 are e.g. potentiometers or switches
Input(s)
Logic

Figure 23 Cross monitoring of input signals and intermediate results

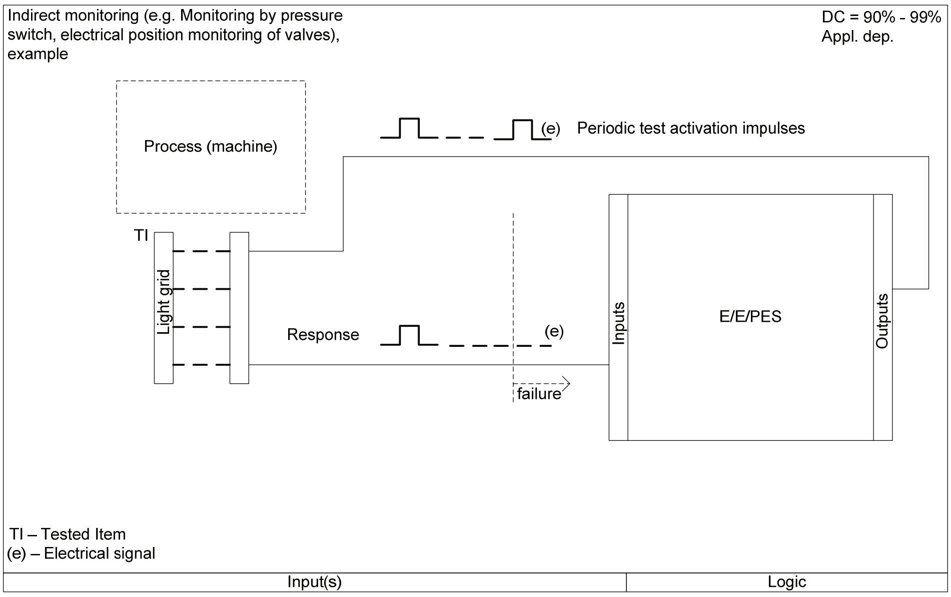


Figure 24 Indirect monitoring

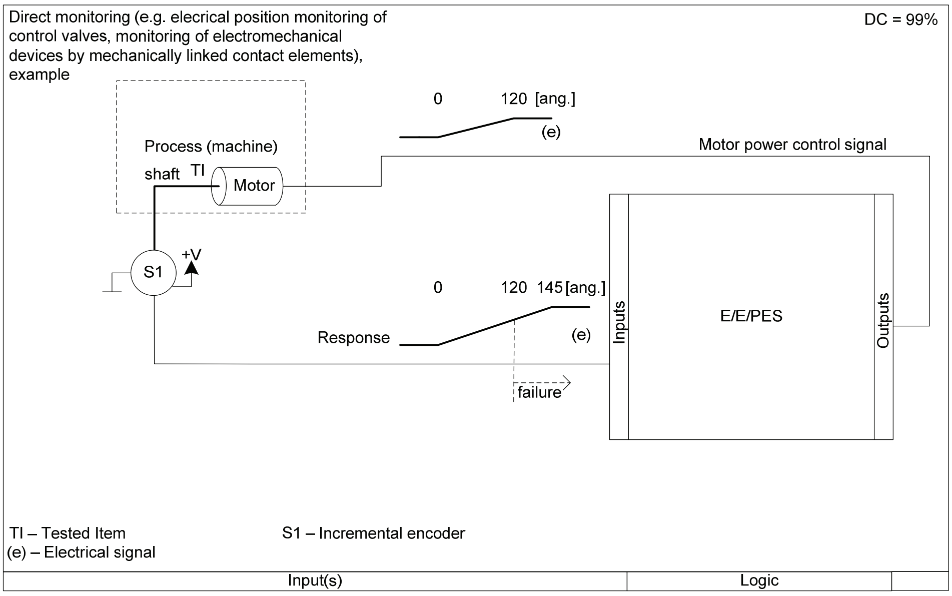

Direct monitoring (e.g. elecrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements), example
DC = 99%
0
120 [ang.]
(e)
Process (machine)
Motor power control signal
shaft
TI
Motor
S1
+V
0
120 145 [ang.]
Response
(e)
Inputs
E/E/PES
Outputs
failure
TI – Tested Item
S1 – Incremental encoder
(e) – Electrical signal
Input(s)
Logic

Figure 25 Direct monitoring

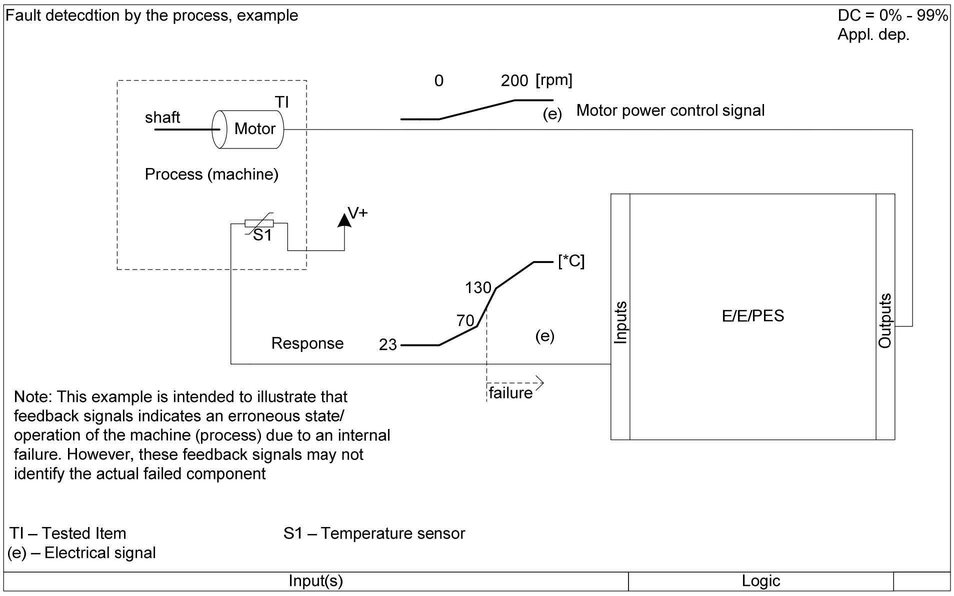

Fault detecdtion by the process, example
DC = 0% - 99%
Appl. dep.
0
200 [rpm]
(e) Motor power control signal
shaft
TI
Motor
Process (machine)
V+
S1
[*C]
130
70
Response
23
(e)
failure
Inputs
E/E/PES
Outputs
Note: This example is intended to illustrate that feedback signals indicates an erroneous state/ operation of the machine (process) due to an internal failure. However, these feedback signals may not identify the actual failed component
TI – Tested Item
(e) – Electrical signal
S1 – Temperature sensor
Input(s)
Logic

Figure 26 Fault detection by the process

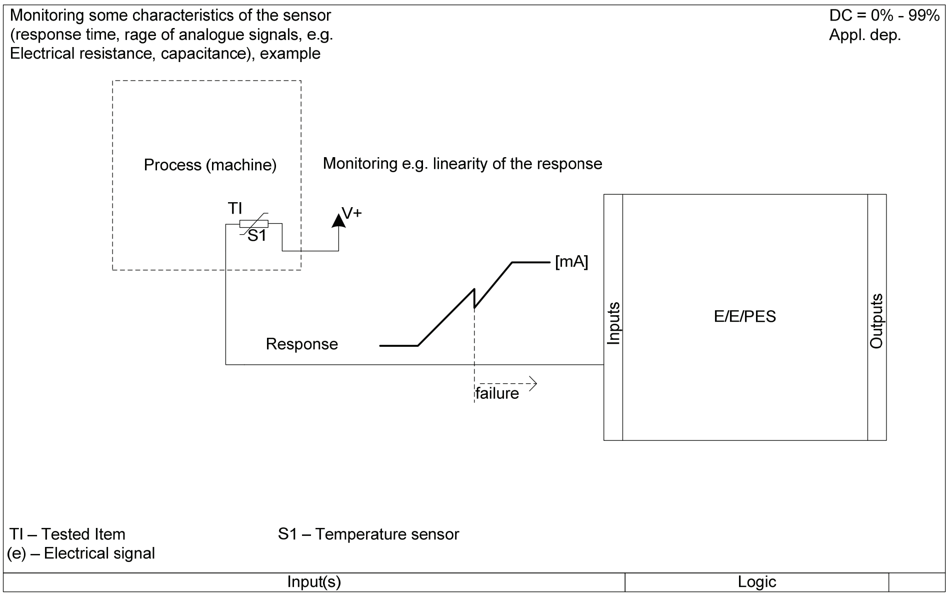
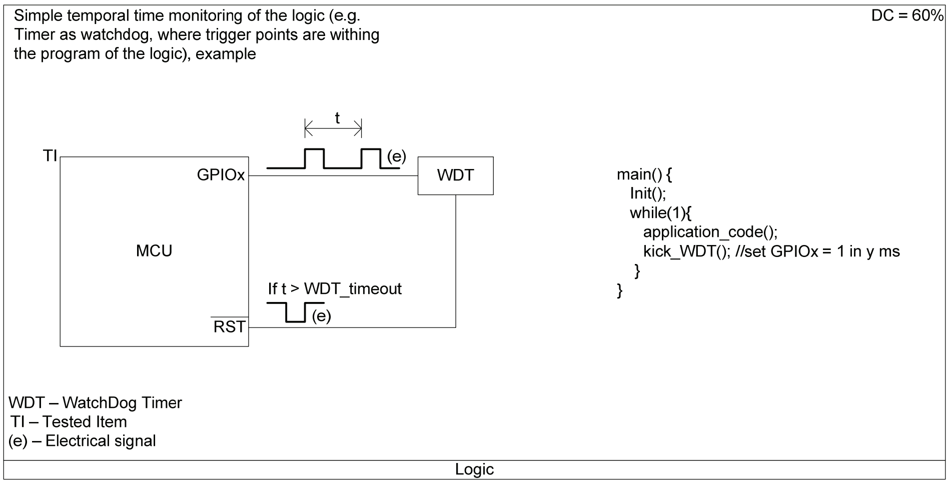
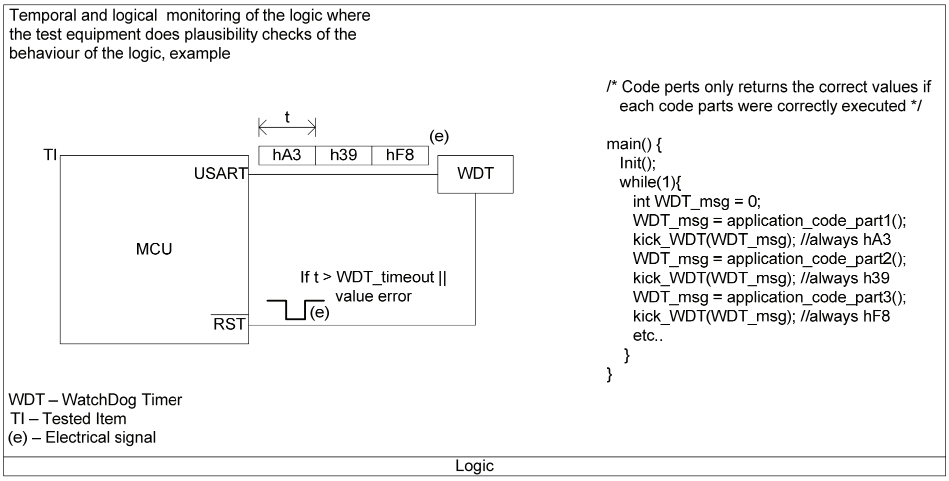

Monitoring some characteristics of the sensor (response time, rage of analogue signals, e.g. Electrical resistance, capacitance), example
DC = 0% - 99%
Appl. dep.
Process (machine)
Monitoring e.g. linearity of the response
TI
S1
V+
[mA]
Response
failure
Inputs
E/E/PES
Outputs
TI – Tested Item
(e) – Electrical signal
S1 – Temperature sensor
Input(s)
Logic

Figure 27 Monitoring some characteristics of the sensor


Simple temporal time monitoring of the logic (e.g. Timer as watchdog, where trigger points are withing the program of the logic), example
DC = 60%
t
(e)
TI
GPIOx
WDT
MCU
If t > WDT_timeout
(e)
RST
WDT – WatchDog Timer
TI – Tested Item
(e) – Electrical signal
Logic

```
main() {
  Init();
  while(1){
    application_code();
    kick_WDT(); //set GPIOx = 1 in y ms
  }
}
```

Figure 28 Simple temporal time monitoring


Temporal and logical monitoring of the logic where the test equipment does plausibility checks of the behaviour of the logic, example
t
(e)
hA3
h39
hF8
TI
USART
WDT
MCU
If t > WDT_timeout || value error
(e)
RST
WDT – WatchDog Timer
TI – Tested Item
(e) – Electrical signal
Logic

```
/* Code perts only returns the correct values if
   each code parts were correctly executed */

main() {
  Init();
  while(1){
    int WDT_msg = 0;
    WDT_msg = application_code_part1();
    kick_WDT(WDT_msg); //always hA3
    WDT_msg = application_code_part2();
    kick_WDT(WDT_msg); //always h39
    WDT_msg = application_code_part3();
    kick_WDT(WDT_msg); //always hF8
    etc..
  }
}
```

Figure 29 Temporal and logic monitoring

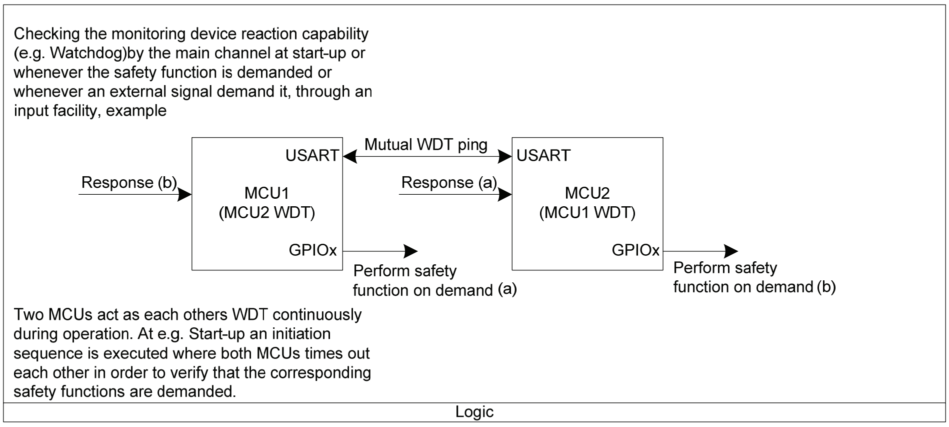

Checking the monitoring device reaction capability (e.g. Watchdog)by the main channel at start-up or whenever the safety function is demanded or whenever an external signal demand it, through an input facility, example
USART
Mutual WDT ping
USART
Response (b)
MCU1
(MCU2 WDT)
Response (a)
MCU2
(MCU1 WDT)
GPIOx
GPIOx
Perform safety function on demand (a)
Perform safety function on demand (b)
Two MCUs act as each others WDT continuously during operation. At e.g. Start-up an initiation sequence is executed where both MCUs times out each other in order to verify that the corresponding safety functions are demanded.
Logic

Figure 30 Checking the monitoring device reaction capability

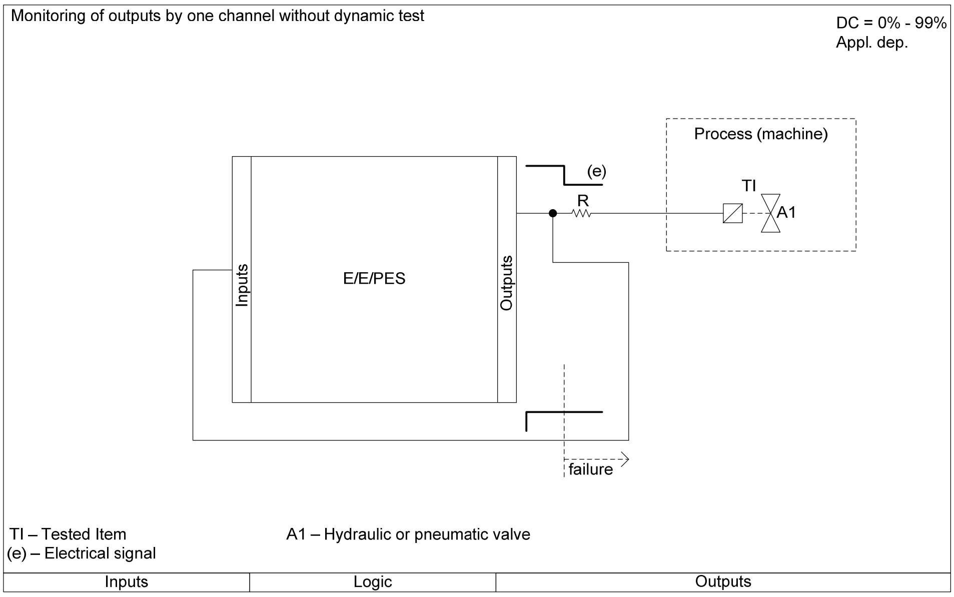


Figure 31 Monitoring of outputs by one channel without dynamic tests

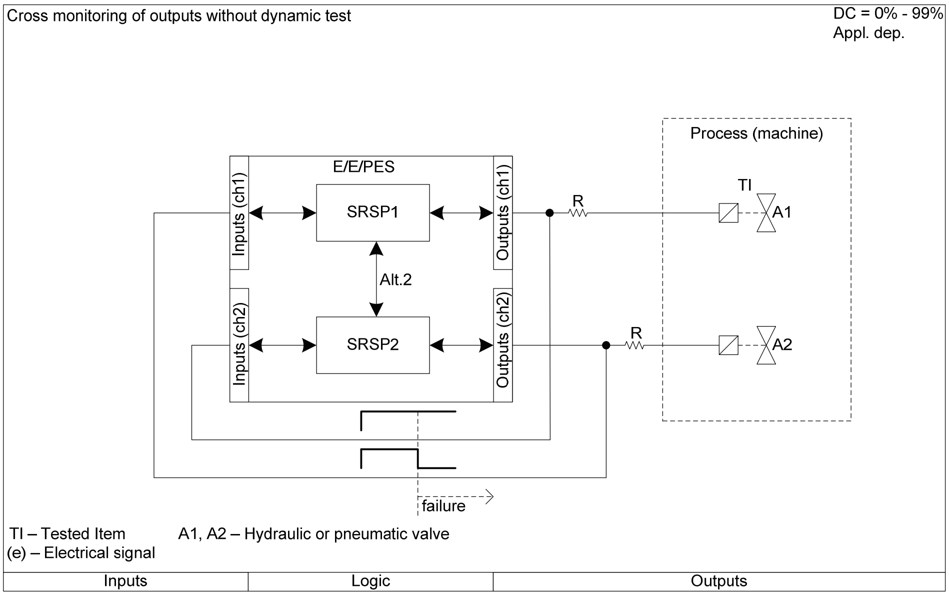


Figure 32 Cross monitoring of outputs without dynamic test

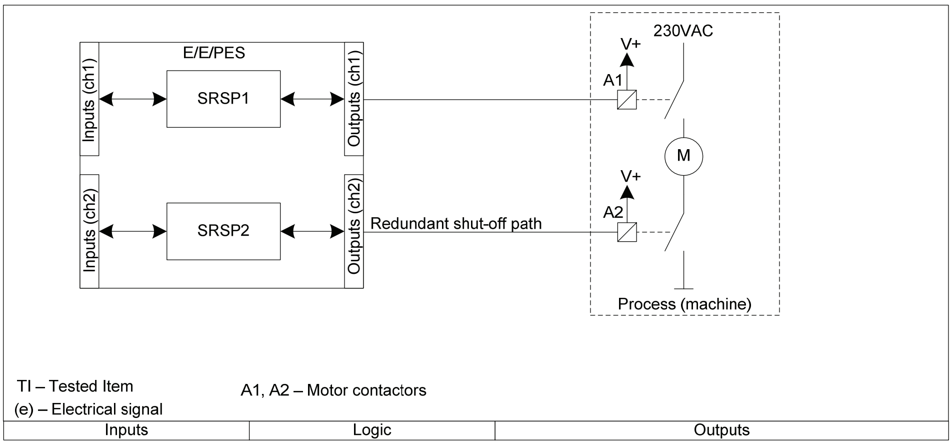


Figure 33 Redundant shut-off path with no monitoring of the actuator

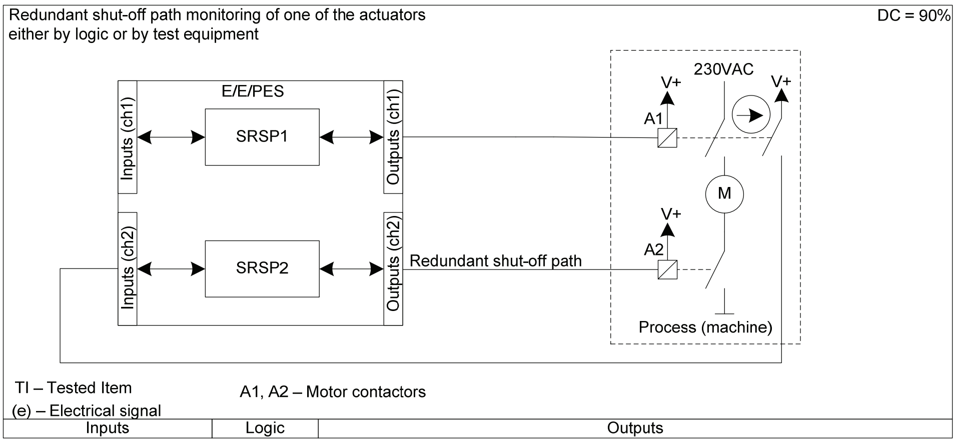


Figure 34 Redundant shut-off path monitoring of one of the actuators

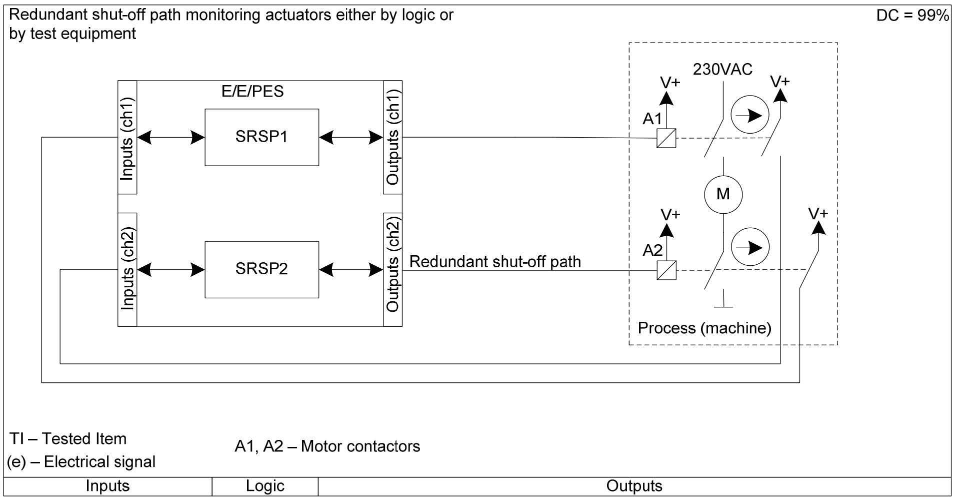


Figure 35 Redundant shut-off path monitoring actuators

SP Technical Research Institute of Sweden

Our work is concentrated on innovation and the development of value-adding technology. Using Sweden's most extensive and advanced resources for technical evaluation, measurement technology, research and development, we make an important contribution to the competitiveness and sustainable development of industry. Research is carried out in close conjunction with universities and institutes of technology, to the benefit of a customer base of about 10 000 organisations, ranging from start-up companies developing new technologies or new ideas to international groups.

SP Technical Research Institute of Sweden
Box 857, SE-501 15 Borås, SWEDEN
Telephone: +46 10 516 50 00
Telefax: +46 33 13 55 02
E-mail: info@sp.se
www.sp.se

SP Electronics
SP REPORT 2011:81
ISBN 978-91-87017-14-8
ISSN 0284-5172

More information about publications published by SP: **www.sp.se/publ**