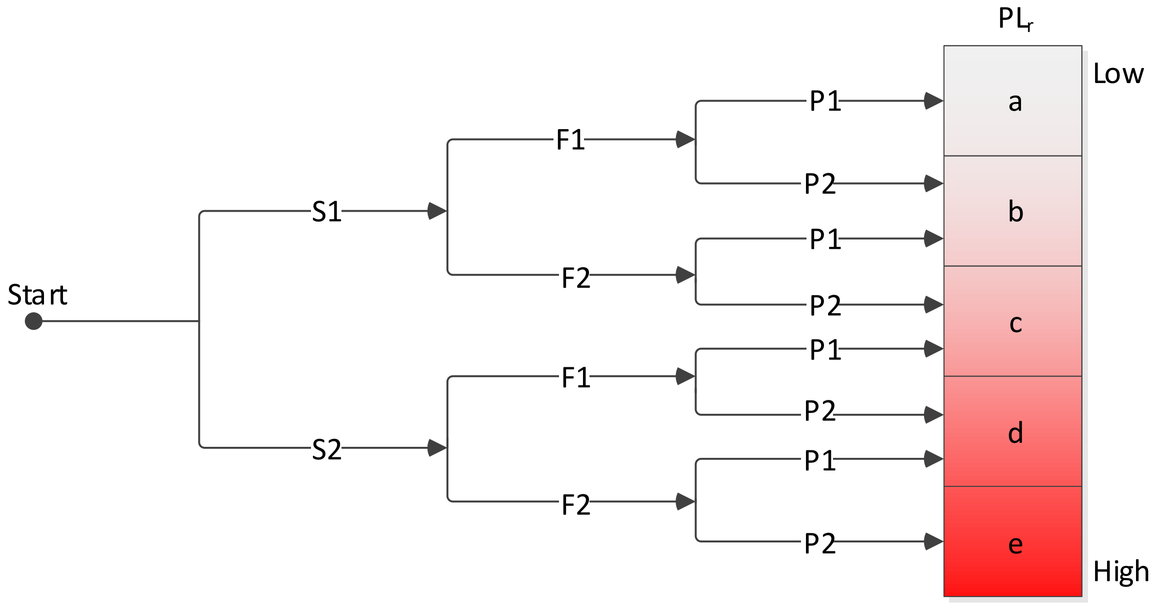
SAFETY AND TRANSPORT
ELECTRONICS



Introduction to Hardware Architecture and Evaluation According to EN ISO 13849-1

Joe Furborg, Andreas Söderberg

RISE Report 2019:13

Introduction to Hardware Architecture and Evaluation According to EN ISO 13849-1

Joe Furborg, Andreas Söderberg

Abstract

Introduction to hardware architecture and evaluation according to EN ISO 13849-1

Hardware realization of safety functions, in safety related machinery control systems can, according to EN ISO 13849-1, be realized as one out of five distinct designated architectures. This report gives examples and guidance for choosing a designated architecture which fulfills the required risk reductive measure of the safety function.

Key words: EN ISO 13849-1, Designated architectures, Safety function, Redundancy, PL

RISE Research Institutes of Sweden AB

RISE Report 2019:13
ISBN: 978-91-88907-37-0
Borås 2019

Content

Table of Figures

Table of Tables

Preface

RISE Research Institutes of Sweden is a notified body for the Machinery Directive. We perform EC Type Approvals of Safety components. RISE is also a notified body of several other directives.

SMP Svenska Maskinprovning is also a part of RISE. SMP is a notified body of many type of machinery.

This report aims to serve as support in the process of evaluating the specification, allocation and implementation of safety functions performed by clients. The standards used for this purpose (e.g. ISO 13849-1:2016) states a limited set of precise requirements on this process. However, these requirements are formulated in such manners that they may be fulfilled by a variety of different technical solutions.

Safety critical systems becomes more and more common in everyday applications/products and are a vital part of any product that complies with the Machinery Directive. Use of safety critical embedded systems has been added by the product developer to minimise the damage to the machine users in the event of a failure of the application.

Quality related aspects such as product cost, performance or other product properties are not addressed by the requirements of EN ISO 13849-1:2016, thus a challenging task for the product developers is to choose/find the most optimal solution with respect of their specific application.

This report is a practical guide for evaluating the hardware architecture together with reliability calculations in accordance to EN ISO 13849-1:2016.

This report should be read as guidance, and not be interpreted as requirements. The requirements can be found in the Machinery directive and in harmonized standards.

Please obtain the full text of EN ISO 13849-1:2016 to know all parts of the standard. Standards are protected by copyright and can be bought from ISO (www.iso.org) or at your national standardizations (e.g. www.sis.se in Sweden).

Summary

This report gives a guidance in applying EN ISO 13849-1:2016 to evaluate the characteristics of a safety function and to find the required performance level of each safety critical system. While also, realize the hardware architecture and to finally calculate the reliability of each safety critical systems.

This report gives examples of:

- *What a Safety function is*
- *What parts of the control system are regarded as safety critical functions*
- *What a safety function should fulfil*
- *What's the characteristics of a reliable safety function*
- *Determining the required performance level of the safety function*
- *Evaluating the achieved performance level of the Safety function*
- *Realizing the safety function as a hardware architecture*
- *Evaluation of the hardware architecture*

1 Functional Safety

Functional safety is a term which consists of reducing risks and limit hazardous events from occurring. There are safety legislations that a manufacturer shall fulfil when designing a product. The background to these safety legislations is the Machinery directive. In this section is the Machinery directive presented, also a risk analysis, followed by what a machinery control system is.

1.1 The Machinery Directive

The Machinery Directive, 2006/42/EC is one of the main legislations of the European Union. The directive provides harmonization of essential health and safety requirements for machinery. The directive informs the manufacturer of certain safety measures which must be fulfilled for the machinery to be approved on the market in the European Union (EU) and the European Economic Area (EEA).

If a machine/product shall be placed on the market within the EU and EEA area, then it must fulfil the requirements of the directive. A machine that fulfils the requirements of the directive is considered to guarantee a high level of protection for EU workers and citizens while promoting a free movement of machinery within the market.

The Machinery Directive, Appendix 1, Clause 1.1.2 states the following requirements for machinery must be fulfilled for a machinery to be considered as safe, also referred to as *safety by design*:

> *Machinery must be designed and constructed so that it is fitted for its function, and can be operated, adjusted and maintained without putting persons at risk when these operations are carried out under the conditions foreseen but also taking into account any reasonably foreseeable misuse thereof.*
>
> *The aim of measures taken must be to eliminate any risk throughout the foreseeable lifetime of the machinery including the phases of transport, assembly, dismantling, disabling and scrapping.*

The directive also has a three successive step approach to fulfil the requirements on machinery safety. The Machinery Directive, Appendix 1, Clause 1.1.2, §174 refer to the three successive step as the *3-step method.*

- First priority – Inherently safe-design measures
  (e.g. use a low-power hydraulic press instead of a high-power one, if possible)
- Second priority – risk reduction by safeguarding and protective measures
  (e.g. install interlocking gates around a robotics cell)
- Third priority – risk reduction by information and warnings
  (e.g. explain that the noise level of a lawn mower requires the user to wear hearing protection)

The order of these steps must be followed when deciding the correct safety measures of the machinery to fulfil the directive. A machinery manufacturer must eliminate all hazards of the machinery before protective measures can be considered. The same principle applies for protective measures, every protective measure must be considered before any warnings or instructions for operators/users can be issued.

1.2 Risk assessment

A risk assessment is a process to state the limits of the product/application and identify, analyse and evaluate if the product/application can cause any harm. The risk assessment is a useful tool to decide the appropriate measures to reduce hazardous situations. The risk assessment shall be performed by the manufacturer of the complete machinery, since the manufacturer has all the information and knows the limitations of the product.

The standards SS-EN ISO 12100 and ISO/TR 14121-2 states that a risk assessment and risk reduction can be performed in the following order:

- Determine the limits of the machinery, which include the intended use and any reasonably foreseeable misuse thereof
  (e.g. state the limitations of the product)
- Identify the hazards and associated hazardous situations and events
  (e.g. go over the complete product thoroughly and identify hazards)
- Estimate the risk for each identified hazardous event
  (e.g. estimate probability of occurrence and severity for each hazardous event)
- Evaluate the risk and take decisions about the need for risk reduction
  (e.g. evaluate whether risk reduction is required)
- Eliminate the hazard or reduce the risk associated with the hazard by means of protective measures.
  (e.g. use the 3-step method to eliminate the risk(s))

The risk assessment is usually performed in different steps starting with setting the limits of the machine. Followed by a general risk assessment covering all risks related to the machine. During this step is the overall product evaluated and potential risks (sources of harm) are highlighted.

The highlighted areas are then analysed and the severity while also the probability of occurrence for each hazardous event is determined. With every risk estimated and evaluated, the risk assessment can be refined into a more detailed risk assessment specifically regarding risks to be reduced by e.g. the means of the control system. It’s the later risk assessment that is relevant for the contents of this report.

1.3 Machinery Control Systems

When designing any type of machine, the manufacturer doesn't only need to consider the machinery, but also a control system. The control system ensures that the machinery operates as intended.

Machinery control systems are usually realized by a combination of software and different physical components such as: electrical, mechanical, hydraulic or pneumatical components, but are not limited to these component types.

The combined system of hardware and software interoperates the input signals to the system and generates an output signal. Forming a so-called ILO-System, Input, Logic and Output -system, se Figure 1. A system with only one input to output correlation is a single channel system. However, there are systems which may have more channels, which are thus called dual-channel or multi-channel systems.

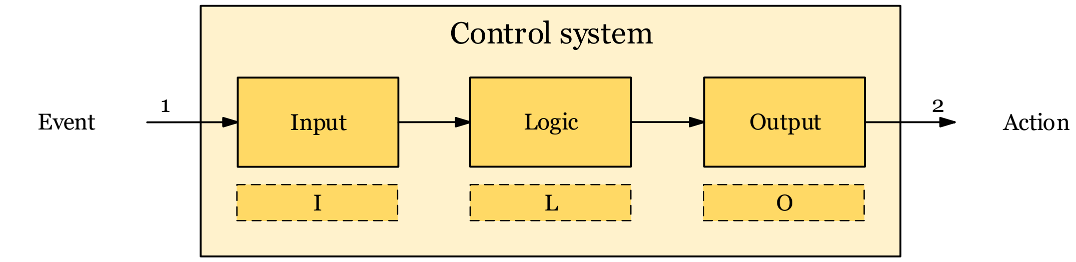


Figure 1 General schematic of an ILO-System

Legend:

I	*Input*
L	*Logic unit*
O	*Output*
1	*Initial event which activates the control functionality*
2	*Output to power control elements*

An example of a ILO-system can be: the activation of a position switch which in turn indicates that an elevator has reached the desired level so that the elevator motor can slow down the elevator and let the passengers get off. Here are the signal from the position switch the input to the processing unit which in turn generates the output signal to the power control elements which will slow down the motor until the elevator stops.

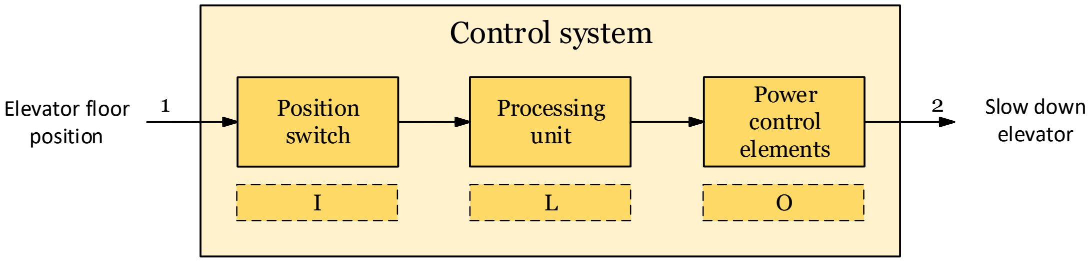


Figure 2 Example of elevator ILO-System

Legend:

I	*Input – Position switch*
L	*Logic unit – Processing unit*
O	*Output – Power control elements*
1	*Event – Elevator reaches a specific floor*
2	*Output action – Turn off power to elevator motor*

The Machinery Directive, Appendix 1, Clause 1.2.1 states requirements that must be fulfilled for a machinery control system. From these requirements it's clear that the design of the control systems is important when constructing any type of machinery and that the control system has an important role regarding the safety of machinery.

> *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.*

The directive also states that 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*

2 Safety functions

Safety functions are functionality implemented in a product/application which sole purpose is to reduce risk(s) by decreasing either the probability of occurrence and/or the severity of hazardous events. The general functionality of safety functions is presented in this section, followed by what safety related parts are and different combinations. Finally, are commercial of the shelf products (COTS), presented and a section regarding the reliability of safety functions.

2.1 Purpose of the safety function

In EN ISO 13849-1:2016, clause 3.1.20 is safety functions defined as:

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

This means that safety functions sole purpose is to reduce risk(s) by decreasing the probability of occurrence and/or the severity of hazardous events. Figure 3 presents a generic safety function. Safety functions may also be been realized together with the ordinary machinery control system. however, this may not always be the case.

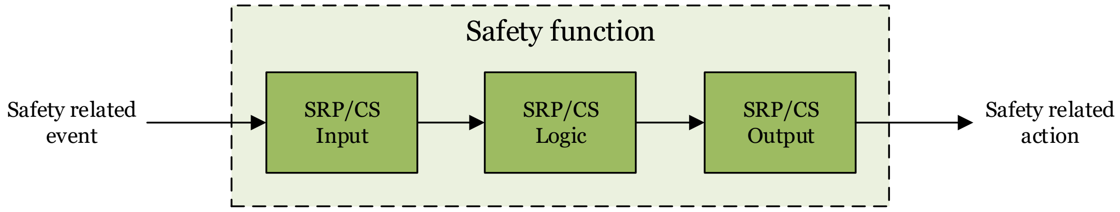


Figure 3 Generic overview of a safety function

In the event of a hazardous situations shall the safety function act to reduce the hazardous event. However, if the hazardous situations can't be eliminated completely, then the safety function shall reduce the severity of the risk as far as possible.

Safety functions may be implemented/realized as inherently safe-design measures or as safeguarding and protective measures. However, each safety function is a implementation of a risk reduction measure from the risk assessment. For this report are safety functions realized by a control system.

There are two modes of operation for a safety function, which are: high demand or continuous mode. In EN ISO 13849-1:2016, clause 3.1.38 are the two modes defined as:

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

This means that a safety function realized in continuous mode will be operating as part of a normal function of the control system. This is typically applicable in machinery with electronical steering, which requires the safety function to be working while the machinery is operating, e.g. forestry machinery, mobile crane steering, steer-by-wire.

High-demand mode of safety function can typically be realized as safeguarding measures such as interlocking gates or presence detection. The safety function reacts on a specific action/event and activates the correct response, e.g. interlock function on the gate to a robot cell, laser-screens at the delivery area of an automatic storage system.

A list of typical safety functions can be obtained in EN ISO 13849-1:2016 clause 5. However, the following list contains some examples of common safety functions:

- Emergency-stop (e.g. E-stop)
- Guarding (Interlocking guards)
- Preventing of unexpected start-up
- Manual reset function
- Presence sensing functions
- Hold-to-run functionality

2.1.1 Safe-state

A safety function can be realized with self-diagnostics, which have the purpose to detect if there are any faults with any parts/components of the safety function. If a fault is detected, then the control system shall initialize an appropriate action. The appropriate action depends on the application, however in most of the machinery cases the appropriate action is to initiate a so called safe-state (e.g. a safety function is performed).

With safe-state means that the machinery is put in such a state where the risk is eliminated (e.g. turning off the power to a machinery/motor thus eliminating the hazardous situation). It may also be applicable to have the safe-state as an alarm to warn others of danger. In some cases, it’s necessary to be able to operate the machinery even though a safe state has been initialized. This can for example be realized as a hold to run functionality, to operate a crane, even though the systems is warning for overweight.

Safe state is not defined in EN ISO 13849-1:2016, however in standard IEC 61508:2010, part 4, Clause 3.1.13 defines safe-state 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)

2.1.2 Safety functions with inherent design

The amount of risk reduction that a safety functions shall provide can vary depending on the design of the machinery. A machinery manufacturer may incorporate inherent safe design measures from the beginning of production of the machinery. Thus, creating a system which doesn't rely as much on safety functions compared to a product which doesn't have inherent design measures from the start.

Depending on the amount of inherent safe design incorporated in the design of the machinery, can different levels of safety functions be implemented/realized for the machinery. Figure 4 presents a general representation on how the same level of risk reduction can be achieved with and more or less incorporated safety design and safety functions.

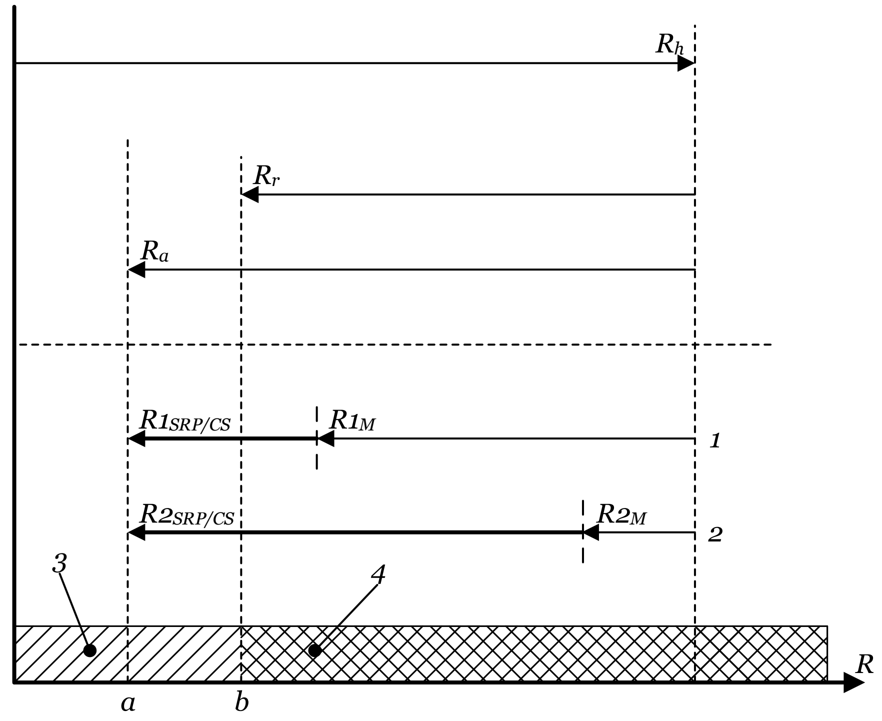


Figure 4 Risk reduction with safety functions and inherent design measures

Legend:

R	*Risk*
R_h	*The risk for a specific hazardous situation, before any protective measures are applied*
R_r	*Risk reduction required from protective measures*
R_a	*Actual risk reduction achieved from with protective measures*
$R2_{SRP/CS}$ $R2_{SRP/CS}$	*Risk reduction achieved from the safety functions with SRP/CS*
$R1_M$ $R2_M$	*Risk reduction achieved from the safety functions with mechanical protection*
1	*Solution 1 major part of risk reduction is performed by protective measures other the SRP/CS (e.g. mechanical protection), small part of risk reduction is due to SRP/CS*
2	*Solution 2 Major part of risk reduction is performed by SRP/CS (e.g. light curtain), small part of risk reduction is due to protective measures (e.g. mechanical protection)*
3	*Adequate risk reductions*
4	*Inadequate risk reductions*
a	*Further risk reduction obtained through solutions 1 and 2*
b	*Adequate risk reduction*

2.2 Safety-related part(s) of a control system

In EN ISO 13849-1:2016-1, clause 3.1.1 defines a safety-related part of a control system (SRP/CS) as:

> *part of a control system that responds to safety-related input signals and generates safety-related output signals*

This means that any part of a control system, which has safety-related input signals which in turn generates safety-related output signals is a so called "Safety-related part of a control system".

The Note 1 to the statement above describes a complete safety function as:

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

This means that any combination of sensor, logic and final output which has safety-related inputs and outputs is a safety function. Safety functions are thus built up by combinations of SCP/CS's. Different safety functions may share the same SRP/CS (e.g. a logic unit, power control element(s)).

Safety functions may also be implemented in the same logic unit together with the ordinary system control functionality. The SRP/CS of a safety function which is implemented together with the ordinary system control functionality can be seen in Figure 5.

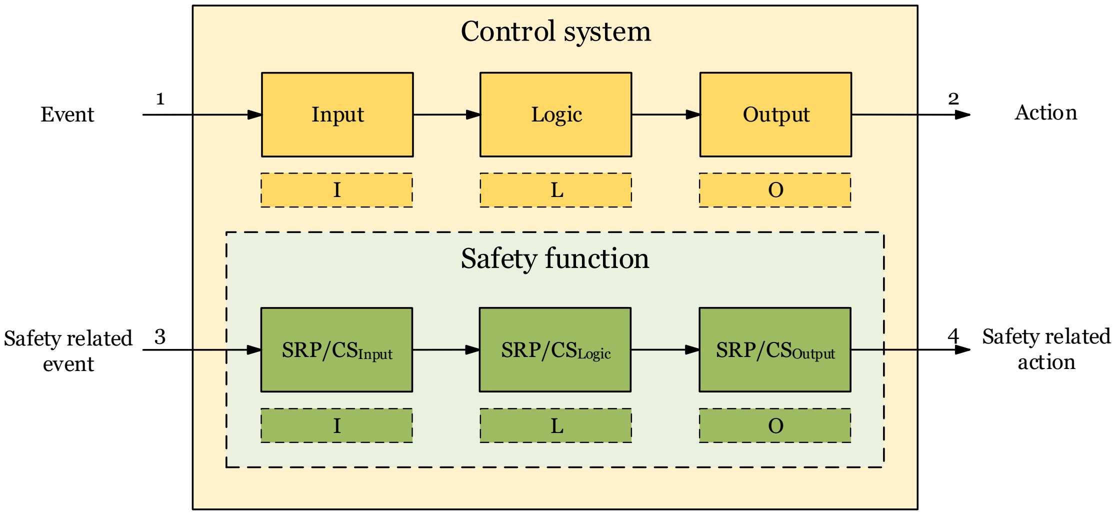


Figure 5 Safety function presented as part of the control system

Legend:

I	*Input*
L	*Logic unit*
O	*Output*
1	*Input to ordinary machinery control which activates control functionality*
2	*Output to machinery functionality*
3	*Initial safety related event*
4	*Safety related output to power control elements*

A failure in any of the hardware components which are considered as SRP/CS for the safety function can cause two possible outcomes. Either will the function of the safety function be lost, or the safety function will be able to continue to work. These two modes are often referred as "*The loss of the safety function*" or as "*the continued performance of the safety function*".

The loss of the safety function means that this safety function will not work if any SRP/CS is faulty. While the continued performance of the safety function means that even if a SRP/CS is faulty, the safety function will still work.

2.2.1 Combinations of SRP/CS

Safety functions are always realized as input, logic and output systems, which have safety related input signal and in turn generates safety related output signals. When realizing a safety function, it's important to identify the individual SRP/CS that fulfils the safety function as seen in Figure 6.

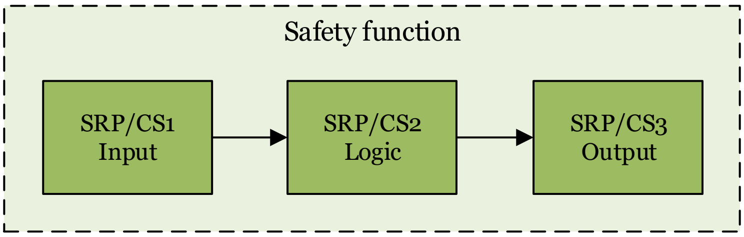


Figure 6 Safety function with separate input, logic and output

However, there are some SRP/CS which have integrated input, logic and output, se Figure 7. These SRP/CS are usually control systems which has been constructed to solve a specific problem.

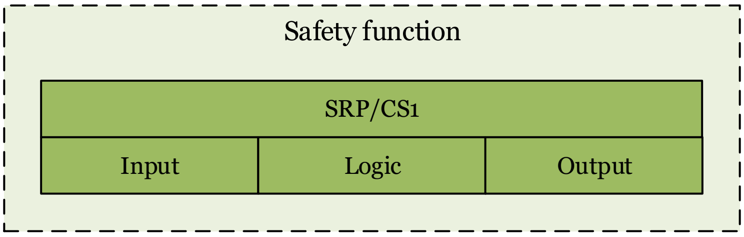


Figure 7 SRP/CS which have integrated input, logic and output

Safety functions can also be a combination of the two options presented above, this can be seen in Figure 8. Where a commercially constructed control system is used together with a SRP/CS$_{\text{Input}}$ component to form the whole safety function.

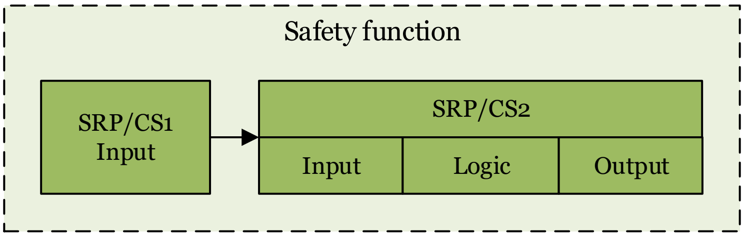


Figure 8 safety function as a combination of SRP/CS

2.2.2 Safety function with several inputs/outputs

One initial hazardous event may not be enough to execute the safety related action. Sometimes it's required that two events occur simultaneously before the safety function executes the safety related action, se Figure 9. Example of this is two-hand hold-to-run, where the user must use both hands to active the machinery.

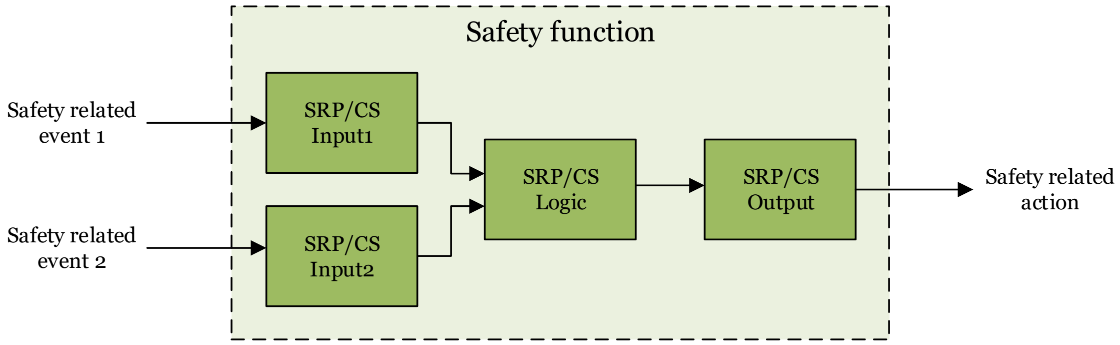


Figure 9 Safety function with two inputs

Safety functions may also affect two different outputs, se Figure 10. Examples of this can be when a grinder has been stopping due to an initial safety related event (e.g. emergency stop has been activated), the conveyer feeding the grinder must also be stopped. So, the grinder isn't overfilled.

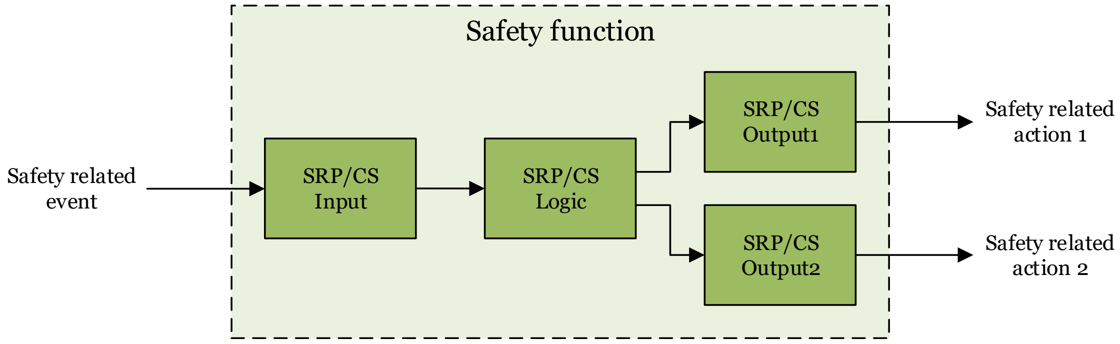


Figure 10 Safety function with two outputs

The same logic unit may also be utilized to serve more than one safety function, se Figure 11. Where, the same logic unit is used for two safety functions.

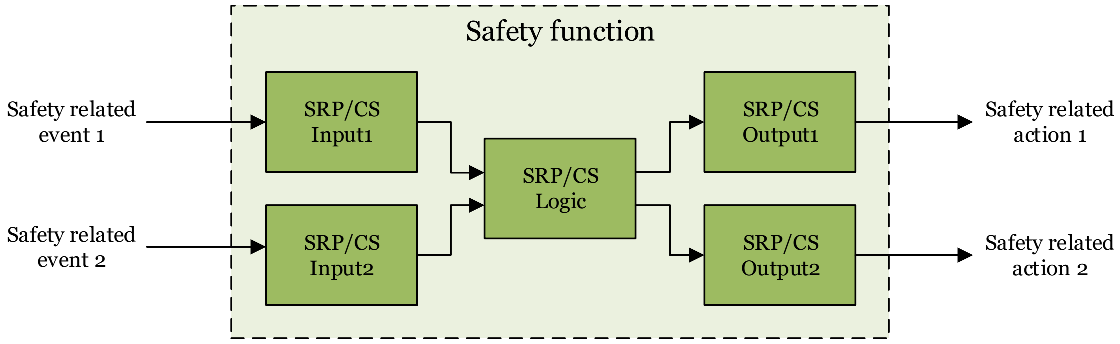


Figure 11 Two safety function realized in the same logic unit

2.3 Safety related commercial-off-the-shelf components

Commercial-off-the-shelf (COTS) are component(s) which have been constructed to solve a specific task. These products are usually constructed in such a way that the user doesn't have to configure the product in order to fit it to the intended application. COTS can be either be a complete software or hardware solution or a combination of software and hardware fitted in one component.

There are COTS which purpose is to solve safety related issues. These components can be used as parts of the safety function or as the whole safety function.

Examples of safety components are, also se Figure 12:

- Presence detection devices
- Gates with microswitches which detects if the gate is open or not
- Emergency stop units
- Two-hand control devices (Dead man's switches)
- Restraint systems to keep persons from getting out of their seats

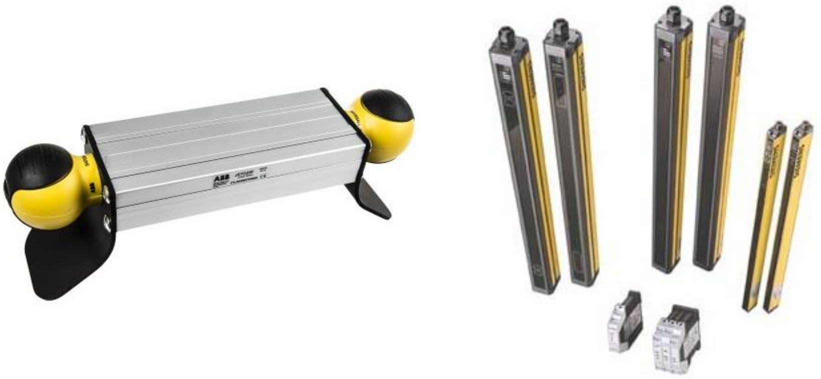


Figure 12 COTS, two-hand control device, light curtains [ABB] [Siemens]

In the machinery directive, Article 2 is a "safety component" defined as a component:

- *which serves to fulfil a safety function,*
- *which is independently placed on the market,*
- *the failure and/or malfunction of which endangers the safety of persons, and*
- *which is not necessary in order for the machinery to function, or for which normal components may be substituted in order for the machinery to function.*

This means that there are COTS components which can be purchased and implemented in an application/product to solve safety related issues. Rather then, designing and constructing a new component to solve the safety related issue.

2.4 Reliability of a safety function

The reliability of a safety function corresponds to the combined reliability of each SRP/CS for the whole safety function. In other words, reliability of safety function, from input signal to output signal, is the combined reliability of each SRP/CS of the whole safety function.

The reliability of a safety function can vary depending on the chosen parts/components. The factors that contribute to reliability of the safety function are the quantified aspects presented in Section 8. Furthermore, can the chosen technology for the safety function also influence the reliability. Due to fault-tolerance of the technology and that the same technical solution for different technologies can have an inherent higher/lower reliability.

There are a couple of ways to enhance the reliability of a safety function, while also reducing the probability of faults of the safety function. This can be done by using "well-tried components" and/or applying well-tried safety principles.

EN ISO 13849-1:2016 defines "Well-tried components" for safety related applications as:

(1) widely used in the past with successful results in similar applications, or
(2) made and verified using principles which demonstrate its suitability and reliability for safety-related applications

The standard also states that newly developed components and safety principles may be considered as equivalent to "well-tried" if they fulfil the conditions of (2).

It's also possible to go through and improve the structure of the safety function, se more about design structures in Section 5.

Safety functions can also be realized as two or more ILO-System's in parallel making the safety function a so-called dual-channel or multi-channel safety function. The overall system redundancy will increase by having two or more systems in parallel. Since in the event of a failure of one of the channels, the other(s) may be unaffected and will still work. Thus, achieving the continued performance of the safety function.

The reliability can be increased by any of the methods stated above or by a combination of the methods. However, some methods might not be applicable for every technology. Another way to increase reliability is to ensure that the system is redundant and/or add fault monitoring of the system.

3 Required risk reduction

Safety functions are risk reduction measures which purpose is to reduce the probability of the hazardous event. The standard EN ISO 13849-1:2016 provides the risk reductive measure of the safety function as performance level (PL) while the required risk reductive measure of the safety function is presented as required performance level (PL_r). This section covers the methodology to estimate the required risk reduction with EN ISO 13849-1:2016.

There are five levels of risk reduction measure available, these levels range from PL_a to PL_e. Where PL_a corresponds to the lowest risk reduction and PL_e corresponds to the highest risk reduction. Each level corresponds to the average probability of dangerous failure per hour (PFH_d) of the SRP/CS and to the extent of the whole safety function. The PFH_d for each level can be seen in Table 1.

Table 1 Performance level (PL), PFH_d

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

3.1 Required performance level

The required risk reduction when designing a safety function depends on the required preventive measure that the safety function shall perform, which is a result from the risk assessment.

The required performance level of a safety function is determined by evaluating the hazardous areas in the risk assessment and determining the parameters which contribute to the hazardous event. The parameters are: Severity of injury (S), Frequency and/or exposure to hazard (F), and Possibility of avoidance or limiting harm (P).

The parameters must be estimated before the required performance level of the safety function can be decided. The contribution of each parameter can be divided in two groups, where each parameter has a high or low contribution.

The severity of injury, S is thus divided into the two groups: slight injuries (S1) (e.g. normally reversible) and serious injuries (S2) (e.g. normally irreversible). Slight injuries consist of bruising and/or lacerations without complications. While serious injuries consist of amputations and fatality.

The frequency and/or exposure of hazard, F is divided into the two groups: Seldom-to-less-often and/or exposure time is short, (F1) and Frequent-to-continuous and/or exposure time is long, (F2). There is no general valid time period between the parameters F1 and F2, however the standard EN ISO 13849-1:2016, Annex A.2.2 gives a couple of explanations on deciding the parameter F.

If a person is exposed to frequent or continuous hazards, then F shall be chosen as F2. It doesn't matter if it's the same person or if it's different persons who are exposed to the hazard. For example, if it's part of the work procedure to manually enter an area, where there are moving parts to change a piece of equipment. Then F shall be chosen as F2. Also, if the frequency of hazard is higher than once per 15 min, then the frequency parameter shall also be chosen as F2.

If the accumulated exposure time is less the 1/20 of the overall operating time and the frequency of hazard is not higher than once per 15 min, then the frequency parameter shall be chosen as F1.

The probability of avoidance or limiting harm, P is a combination of two factors: the probability of avoiding the hazard and the probability of occurrence of a hazardous event. By evaluating these two factors can a corresponding P be chosen as either P1 or P2. In general, if there exists a chance of avoiding the hazard or if it's possible to reduce the probability of the hazardous event effect significantly, then P1 can be chosen, otherwise chose P2.

The probability of avoiding the harm is affected if a hazardous event can be detected before it can cause harm or if it can be avoided. Factors which are important are: how quickly the hazardous event arises, if it's possible to escape from the hazardous event, are the operating personnel well informed and educated for the equipment, are there practical safety experiences relating to the process present, it the process operated with or without supervision.

The probability of occurrence of the hazardous event has other affecting factors which relate to reliability data and historical accidents on comparable machines or equipment. With comparable machines or equipment means situations where the safety function shall reduce similar or the same risk(s), the same process and operation action and apply to the same technology causing the harm. Human interaction and technical failures are also two factors to consider when deciding the probability of occurrence of the hazardous event.

The final required performance level of a safety function can be decided with the parameters evaluated together with Figure 13. Where the combination of the parameters S, F and P will correspond to a required performance level of the safety function.

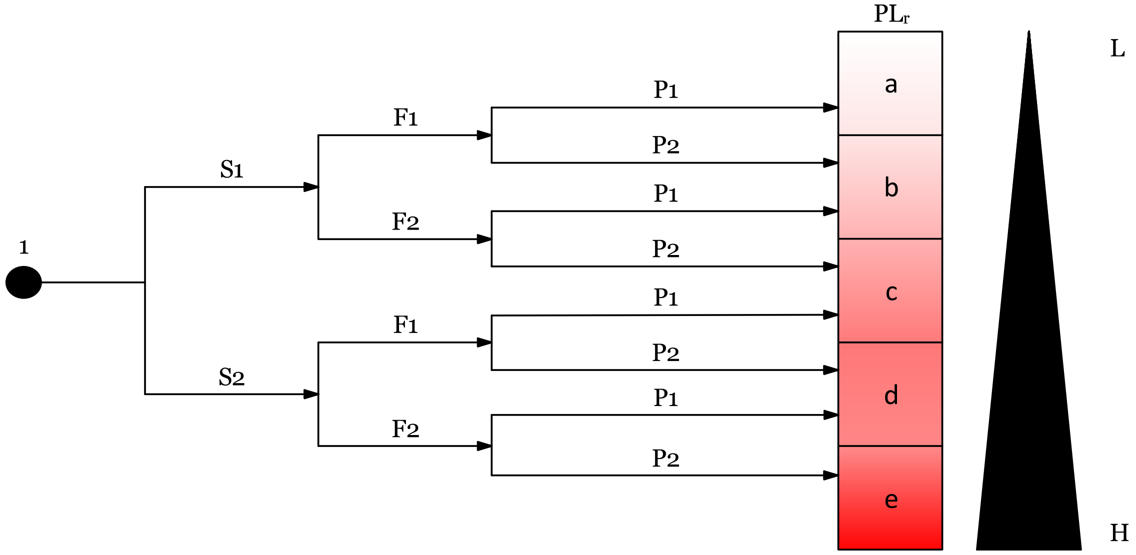


Figure 13 Determining the required PLr for a safety function

Legend:

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*
S	*Severity of injury*
S_1	*Slight (normally reversible injury)*
S_2	*Serious (normally irreversible injury or death)*
F	*Frequency and/or exposure to hazard*
F_1	*Seldom-to-less-often and/or exposure time is short*
F_2	*Frequent-to-continuous and/or exposure time is long*
P	*Possibility of avoiding hazard or limiting harm*
P_1	*Possible under specific conditions*
P_2	*Scarcely possible*

4 Characteristics of risk reduction

Each component in a safety function has different characteristics which affects the overall reliability of the safety function. This section defines the characteristics which are used to evaluate the risk reduction measure that a safety function fulfils. First are mean time to dangerous failures ($MTTF_d$), presented followed by diagnostic coverage (DC) and finally is common cause failures (CCF) presented.

4.1 Mean time to dangerous failure

Mean time to dangerous failure is an estimate of time between failures of a component/function which causes a dangerous failure. $MTTF_d$ is commonly used to estimate the reliability of mechanical and electrical components.

The $MTTF_d$ is divided into three levels which are presented in Table 2. Each level corresponds to the time between dangerous failures. Each channel of the safety function shall be evaluated individually and have a designated $MTTF_d$.

The maximum $MTTF_d$ a channel can achieve is 100 years. If a channel achieves more than 100 years, then it's set to 100 years. For a category 4 (See section 5.5 regarding design categories) the maximum $MTTF_d$ for each channel is 2500 years.

Table 2 Levels of MTTFd [EN ISO 13849-1:2016, table 4]

$MTTF_d$	
Denotation	Range
Low	$3\ years \leq MTTF_d < 10\ years$
Medium	$10\ years \leq MTTF_d < 30\ years$
High	$30\ years \leq MTTF_d \leq 100\ years$

EN ISO 13849-1:2016 states that there are three ways to acquire the $MTTF_d$ for a SRP/CS. The $MTTF_d$ can either be acquired by:

a) *Use manufacturers data*
b) *Use methods in Annex C and Annex D in the standard*
c) *Choose 10 years*

Note: Annex C covers $MTTF_d$ for single components, se sections 4.1.1, 4.1.2 and 4.1.3 and Annex D covers $MTTF_d$ for each channel of the safety function, se section4.1.4.

4.1.1 Acquire the MTTF_d for single electrical components

In the datasheet of the part/component, can the manufacturer state the MTTF_d for electrical components. Sometimes is the failure rate (Λ_D), of the component stated, which can be used to estimate MTTF_d from Equation (1). The failure rate is an estimation of failures in time (FIT). A failure rate of 1 FIT corresponds to a probability of failure which equals to $1 * 10^{-9}$ [Hours].

$$MTTF_d = \frac{1}{\Lambda_D}[hours] \qquad (1)$$

The standard presents some MTTF_d data for some standard electrical parts/components, this can be found in table C2 in EN ISO 13849-1:2016, Annex C. However, if no reliability data can be found for a part/component then 10 years can be used as MTTF_d. For complex components such as integrated circuits shall the reliability data be estimated by using reliability programs such as ITEM ToolKit.

4.1.2 Acquire the MTTF_d for single hydraulic components

Mechanical components must fulfil the general requirements stated in EN ISO 13849-1:2016, Annex C.2 as well as the requirements from Annex C.3 and C.4 to use an estimated value of MTTF_d=150 years. If the mean number of annual operations (n_{op}), are lower than 1 000 000 then, the MTTF_d can be estimated from Table 3 below. If a hydraulic component doesn’t fulfil the requirements in C.3 then the manufacturer must present values of the MTTF_d in the datasheets.

Table 3 MTTF_d estimation for hydraulic components [EN ISO 13849-1:2016, Annex C, Table C.1]

MTTF_d – Hydraulic components	
Mean number of operations, n_{op} [Cycles per year]	MTTF_d [Years]
$n_{op} \geq 1\,000\,000$	150
$1\,000\,000 > n_{op} \geq 500\,000$	300
$500\,000 > n_{op} \geq 250\,000$	600
$250\,000 > n_{op}$	1200

It’s also possible to estimate the MTTF_d using the B_{10D}-Concept presented in section 4.1.3 rather than using the fixed numbers from Table 3. Provided that the manufacturer presents the data required for the estimation.

4.1.3 Acquire the $\mathrm{MTTF_d}$ for single mechanical, pneumatic and electromechanical components

The $\mathrm{MTTF_d}$ for pneumatic, mechanical and electromechanically components aren't usually presented in the datasheets. Component manufacturer are rather presenting the mean number of operations until 10% of the parts/components fail dangerously ($\mathrm{B_{10D}}$) instead of $\mathrm{MTTF_d}$.

EN ISO 13849-1:2016 provides a concept to estimate the $\mathrm{MTTF_d}$ from the $\mathrm{B_{10D}}$. However, the components must fulfil the requirements in EN ISO 13849-1, Annex C.2 as well as the requirements from Annex C.4.1 to be able to use the $\mathrm{B_{10D}}$-Concept to estimate the $\mathrm{MTTF_d}$.

If all requirements are met, then the $\mathrm{MTTF_d}$ can be calculated by using both $\mathrm{B_{10D}}$ and the mean number of operations $\mathrm{n_{op}}$, see equation (2).

$$MTTF_d = \frac{B_{10D}}{0{,}1 * n_{op}} \tag{2}$$

The mean number of operations $\mathrm{n_{op}}$, can be derived from equation (3).

$$n_{op} = \frac{d_{op} * h_{op} * 3600[s/h]}{t_{cycle}} \tag{3}$$

Where:

d_{op} is the mean number of operations, in days per year
h_{op} is the mean number of operations, in hours per day
t_{cycle} is the mean operation time between the beginning of two successive cycles of the component.

To be able to get an estimation of $\mathrm{MTTF_d}$ from the $\mathrm{B_{10D}}$-Concept it's necessary that either $\mathrm{n_{op}}$ or the components of $\mathrm{n_{op}}$ (i.e. $\mathrm{d_{op}}$, $\mathrm{h_{op}}$ and $\mathrm{t_{cycle}}$) are estimated.

4.1.4 Estimation of the $\mathrm{MTTF_d}$ for each channel

The $\mathrm{MTTF_d}$ can be estimated for each channel of the safety function when the designated architecture has been decided and SRP/CS identified. Each components of the safety function are grouped into different blocks depending on if the component belongs to the Input-, Logic- or Output-part of an ILO-System.

The resulting block groups are a representation of Input-Logic-Output of simplified reliability block diagrams. The connection from input-logic-output is a so-called channel. Where every component within the safety function is part of the channel. This results in that every designated architecture can be described as either single or double channeled, se Table 4.

Table 4 Designated architectures with channel representation

Designated architecture	Channel representation
Category B	Single channel
Category 1	Single channel
Category 2	Single channel
Category 3	Double channel
Category 4	Double channel

The accumulated $\mathrm{MTTF_d}$ for an entire channel, excluding the diagnostics units, can be obtained by equation (4).

$$\frac{1}{MTTF_d} = \sum_{i=1}^{\tilde{N}} \frac{1}{MTTF_{d,i}} = \sum_{j=1}^{\tilde{N}} \frac{n_j}{MTTF_{d,j}} \tag{4}$$

Where:

j is the component typ
$\tilde{N}$ is the number of different component types within the channel
n_j is the number of components of type j within the channel
$\mathrm{MTTF_{d,j}}$ is the $\mathrm{MTTF_d}$ value for the particular component type j

4.2 Diagnostic coverage

Diagnostic coverage is a measure of how well a system can detect and handle faults. The detection of faults is performed by an automatic diagnostic test, which must be implemented/realized together with the safety function either built-in or as a separate unit.

There are four achievable levels of DC available for each SRP/CS, as seen in the Table 5. The higher levels are preferable due to reliability purposes.

Table 5 Diagnostic coverage [EN ISO 13849-1:2016, table 5]

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

A system with a high DC can for example, have fault monitoring of different parts in an ILO-system. Figure 14, shows an example of an ILO system with a separate monitoring unit. This system can for instance have different reactions depending on which part of the control systems that's faulty.

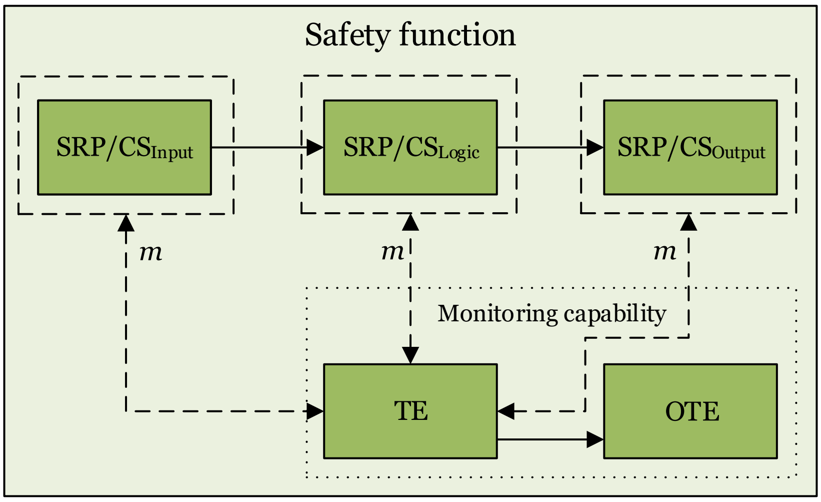


Figure 14 ILO-System with fault monitoring

Legend:

I	*Input*
L	*Logic unit*
O	*Output*
m	*Monitoring*
TE	*Test equipment*
OTE	*Output* of test equipment

4.2.1 Estimation of DC

EN ISO 13849-1:2016, Annex E, and EN61508-4 describes DC as a ratio between the failure rate of detected dangerous failures and the failure rate of total dangerous failures, this means that the DC can be derived from Equation (5). The diagnostic coverage can be estimated from a failure mode and effects analysis (FMEA), se section 9.1. The estimation can be used on a whole system or on subsystems.

$$DC = \frac{\sum \Lambda_{dd}}{\sum \Lambda_d} \ [\%] \tag{5}$$

Where:
$\sum \Lambda_d$ is the probability of total dangerous failures (e.g. the loss of the safety function)
$\sum \Lambda_{dd}$ is the probability of detected dangerous failures (e.g. the total dangerous failure rate of the SRP/CS which is detected and handled by an automatic diagnostic test)

4.2.2 Estimation of DC$_{avg}$ for the whole safety function

Complex system can consist of different diagnostic measures for fault detection. Each diagnostic measure can check different parts of the SRP/CS.

A simplified method to estimate the average diagnostic coverage (DC$_{avg}$) for the entire SRP/CS is presented in equation (6).

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d,1}} + \frac{DC_2}{MTTF_{d,2}} + \cdots + \frac{DC_n}{MTTF_{d,n}}}{\frac{1}{MTTF_{d,1}} + \frac{1}{MTTF_{d,2}} + \cdots + \frac{1}{MTTF_{d,n}}} = \frac{\sum_{n=1}^{k} \frac{DC_n}{MTTF_{d,n}}}{\sum_{n=1}^{k} \frac{1}{MTTF_{d,n}}} \tag{6}$$

The diagnostic coverage and MTTF$_d$ for each component of the SRP/CS is summed up and taken into account when estimating the DC$_{avg}$. Even components without fault detection, DC = 0, are considered and contributes only to the denominator part of DC$_{avg}$.

4.3 Common cause failure

Common cause failures are faults which can affect two channels of a control system simultaneously, se Figure 15. Meaning that safety functions with redundant channels can still be lost if the system is not designed to handle CCF. Examples of CCF can be: Short-circuit, power-loss, unnormal operating temperatures and humidity while also electromagnetic interference.

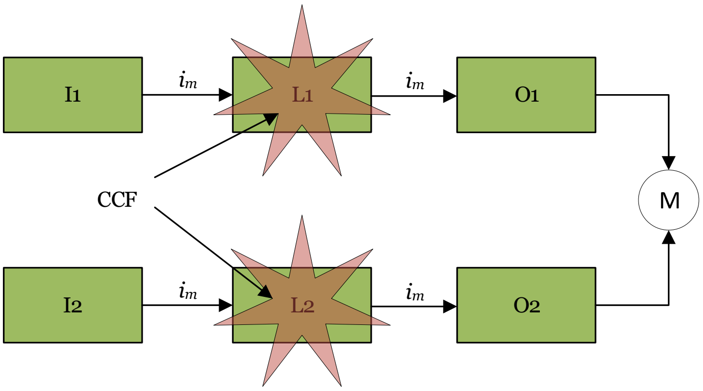


Figure 15 Example of common cause failures

4.3.1 Estimation of CCF

The standard EN ISO 13849-1:2016 provides a process to estimate how well the entire system can handle CCF. This is done by judging how well the safety function is designed with regard to different design areas.

The judging is performed by scoring point depending on if the system fulfils different measures against CCF. When scoring is either full points given or zero points. A safety function which fulfils all measures within each area will receive full points and if an area is only partial fulfilled, then zero points are given.

The scoring for each area can be seen in Table 6. A safety function is required to achieve a minimum of 65 points or better. For a more detailed description of estimation of CCF, see EN ISO 13849-1:2016, Annex F.

Table 6 Scoring table for CCF [EN ISO 13849-1:2016, Table F.1]

NO	Measure against CCF	Score
1	Physical separation between signal paths	15
2	Different technologies/design or physical principles are used,	20
3.1	Protection against over-voltage, over-pressure, over-current, over-temperature, etc.	15
3.2	Components used are well-tried.	5
4	Assessment/analysis	5
5	Competence/training	5
6.1	Environmental: EMC	25
6.2	Environmental: Other influences	10
	Total:	[Max 100]

5 Designated architecture

EN ISO 13849-1:2016 defines five distinct designated architectures of SRP/CS for implementing/realizing a safety function. The categories range from B, 1, 2, 3 and 4 where category B represent the basic architecture with the least fault tolerance and category 4 represent the designated architecture with the highest fault tolerance. A higher designated architecture will also affect the hardware allocation of the SCRP/CS, adding redundancy and increasing the reliability of the safety function.

Each designated architecture specifies the required behaviour of the SRP/CS and its fault tolerance. The basic structure of each category is often similar however, the higher categories have additional components. The categories are the basic parameters to determine the achieved performance level of a safety function. This section will cover the five designated architectures and the characteristics of each architecture.

5.1 Category B

Category B represent the basic designated architecture with the least fault tolerance. A schematic overview of category B is presented in Figure 16. This can be realized as a single input, logic and output channel.

A Category B shall be, as a minimum, designed, constructed, selected, assembled and combined such that the combined safety function fulfils relevant standards and uses "basic safety principles". Furthermore, it's required that the architecture can withstand:

- The expected operating stress for the product
- External influences such as mechanical vibration, electromagnetic interference, dust, power supply interruptions or disturbances.

If there occurs a fault of any parts of this category the safety function might be lost. Also, there are no diagnostic coverage, so the system will not detect if any faults occurs. The $MTTF_d$ is low to medium and common cause failures are not relevant. The maximum PL that this category can achieve is PL = b.

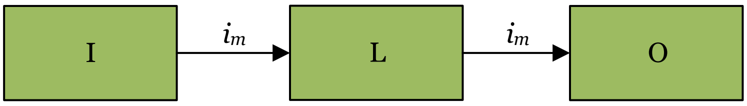


Figure 16 Designated architecture for category B [EN ISO 13849-1:2016, Figure 8]

Legend:

I	*Input*
L	*Logic unit*
O	*Output*
i_m	*Interconnecting means*

5.2 Category 1

Category 1 designated architecture have the same requirements as category B, however a category 1 designated architecture shall use “well-tried” components and “well-tried” safety principles.

If there occurs a fault of any parts of this category the safety function might be lost, however a category 1 structure shall have a $\mathrm{MTTF_d}$ as high, which means that this category is less likely to lose the safety function in the event of any failures.

Furthermore, for this category is the no diagnostic coverage, so the system will not detect if any faults occurs and common cause failures are not relevant. The maximum performance level that this designated architecture can achieve is PL = c. A category 1 architecture is also a single channel, ILO-system such as Category B and can be represented as in Figure 17.

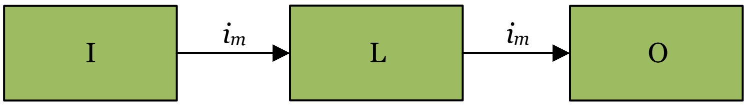


Figure 17 Designated architecture for category 1 [EN ISO 13849-1:2016, Figure 9]

Legend:

I	Input
L	Logic unit
O	Output
i_m	Interconnecting means

5.3 Category 2

A Category 2 designated architecture has the same requirements as category B as well as the “well-tried” requirements from category 1. In addition, a category 2 designated architecture also needs to be able to perform a function check of the safety function.

The function check shall be performed by additional monitoring components. The additional components are: test equipment (TE) with a designated output (OTE). The TE and OTE are implemented together with the safety function in the control system. EN ISO 13849-1:2016 states that TE can be integrated in the same logic unit as the safety function, however this is not required. The OTE must however be separated from the functional channel of the safety function.

In the event of a single fault of the safety function, shall the TE detect the fault and initiate an appropriate control action through the OTE. This means that a category 2 is a single channel ILO-system with monitoring of the functional channel compared to category b and 1. The standard EN ISO 13849-1:2016 states that hazardous situations shall not arise when the control system performs a function check. However, the safety function might be lost between checks.

EN ISO 13849-1:2016 states that the function check shall be performed either within given intervals or at specified occasions. The intervals and specified occasions where the control system shall initialize the function check are:

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

During the function check shall the control system either:

- *allow operation if no faults have been detected, or*
- *generate an output (OTE) which initiates appropriate control action, if a fault is detected.*

The diagnostic coverage for a category 2 design shall at least be low, so the system can detect if faults occurs. The MTTF_d can range between low to high depending on the PL_r. Measures against common cause failures between the safety function and the monitoring units shall have been applied.

The maximum achievable performance level with this design category is PL = d. However, for a category 2 to reach PL = d it’s required that OTE initiates a safe state which is maintained until the fault is cleared. For PL = a, b or c it’s not required that OTE initiates a safe state (which is maintained until the fault is cleared), however whenever practical shall that be the case. In some applications its more practical that the OTE outputs a warning.

Figure 18 shows a category 2 safety function with TE and OTE. The dashed lines between L and TE, shows that L and TE can be realized in the same logic unit. However, the OTE must be separated from the functional channel of the safety function.

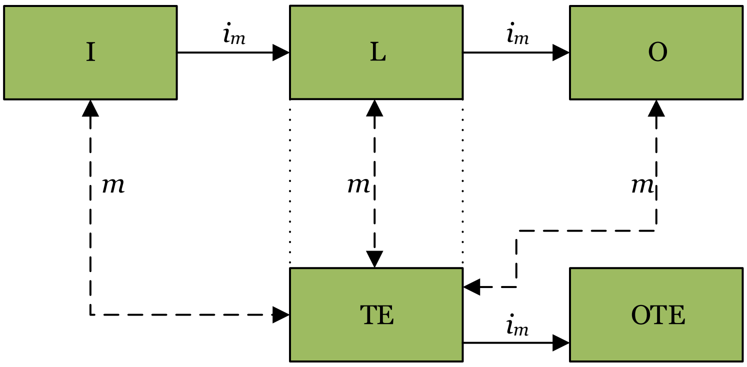


Figure 18 Designated architecture for category 2 [EN ISO 13849-1:2016, Figure 10]

Legend:

I	*Input*
L	*Logic unit*
O	*Output*
i_m	*Interconnecting means*
m	*Monitoring*
TE	*Test equipment*
OTE	*Output* of test equipment

5.4 Category 3

A category 3 designated architecture has the same requirements as a category B as well as the “well-tried” requirements from category 1. In addition, a category 3 designated architecture shall also be able to detect single faults and a single fault shall not lead to the loss of the safety function. Any fault shall be detected either when it occurs or before the next initiation of the safety function.

The main difference between a category 3 and a category 2 is that a category 3 consists of two systems in parallel, making it a redundant system. This ensures that the safety function will continue to perform in the event of a single fault of any parts of the safety function.

The diagnostic coverage shall at least be low, meaning that it can detect some faults, but not all of them. A lot of undetected faults may lead to the loss of the safety function.

The MTTF$_d$ can range between low to high depending on the PL$_r$. Measures against common cause failures shall have been applied. The maximum performance level of a category 3 design structure is PL = d. The schematic overview of a category 3 safety function can be seen in Figure 19.

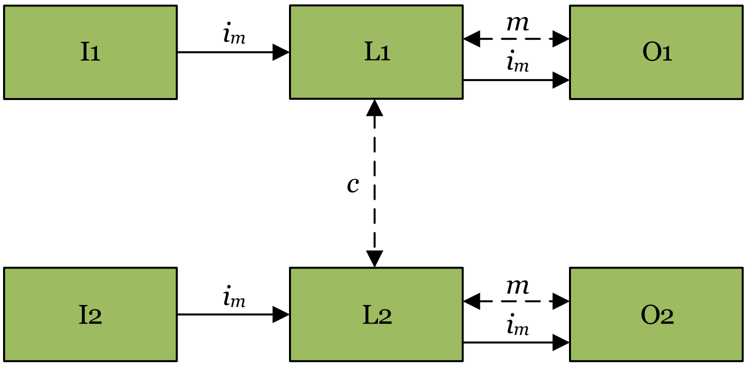


Figure 19 Designated architecture for category 3 [EN ISO 13849-1:2016, Figure 11]

Legend:

I1, I2	*Input*
L1, L2	*Logic unit*
O1, O2	*Output*
i_m	*Interconnecting means*
m	*Monitoring*
c	*Cross monitoring*

5.5 Category 4

A category 4 designated architecture has the same requirements as a category B as well as the "well-tried" requirements from category 1. Faults of a category 4 design shall not lead to the loss of the safety function. In addition, shall single faults be detected at or before the next demand of the safety function.

The differences when comparing category 3 and 4 designs are that accumulated undetected faults shall not lead to the loss of the safety function for a category 4 designated architecture. Furthermore, faults shall be detected in time so that the safety function is never lost.

For a category 4 designated architecture shall the diagnostic coverage be high. While the MTTF_d shall be high for both channels. Measures against common cause failures shall have been applied. This category can achieve a maximum performance level of PL = e. There are two systems in parallel, making it a redundant system, as in the case of category 3. The schematic overview of a category 4 safety function can be seen in Figure 20.

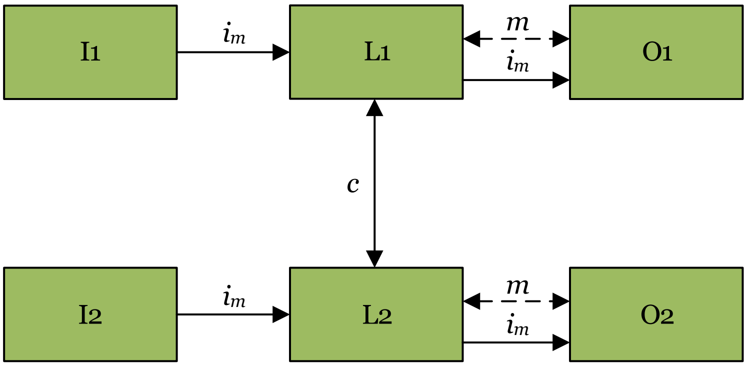


Figure 20 Designated architecture for category 4 [EN ISO 13849-1:2016, Figure 12]

Legend:

I1, I2	*Input*
L1, L2	*Logic unit*
O1, O2	*Output*
i_m	*Interconnecting means*
m	*Monitoring*
c	*Cross monitoring*

6 Software

The software of a control system ensures that the machinery operates as intended. Earlier types of machinery had more functionality which did not depend on software to operate. However, more and more everyday applications have software implemented in the control system to solve operational tasks. This is also true for safety critical systems, such as safety functions. A complete safety function usually consists of both hardware and software, where the software is implemented the Logic-part of the ILO-system. This section covers the software requirements of safety related control systems.

6.1 Safety-related software requirements

There are software requirements stated in EN ISO 13849-1:2016. These requirements ensure that the software can both handle faults introduced by the software developer and by hardware failures in external components. The standard states that the software shall be readable, understandable, testable, and maintainable. Furthermore, the software must be coded in such a way that a person that wasn't involved in the development of the code, shall be able to read and understand the code. Therefore, it's required that the software developer carefully documents the development of the software.

Safety related machinery software is usually divided into two groups, which are safety-related embedded software (SRESW) and safety related application software (SRASW). The main difference between these two types of software is that a machinery-user usually can't access the embedded software. While in some cases it's possible for the user to make adjustments to the machinery in the application software.

Any software implemented into a safety function shall be verified and validated that it fulfils the specification of the safety function. Any changes to an existing safety-related software will make the software certification of the product/application invalid. Therefore, it's required that every change to the software of a safety function is well motivated and carefully thought out. The version number of the software will be updated with any changes to the software.

6.2 Verification and validation

EN ISO 13849-1:2016 presents a recommended V-model for verification and validation of the software. The V-model can be seen in Figure 21. The difference between verification and validation can be described as: *Verification* – "are we building the system right" and *Validation* "are we building the right system". The process of verification and validation is an iterative process which should be perform throughout the entire software development.

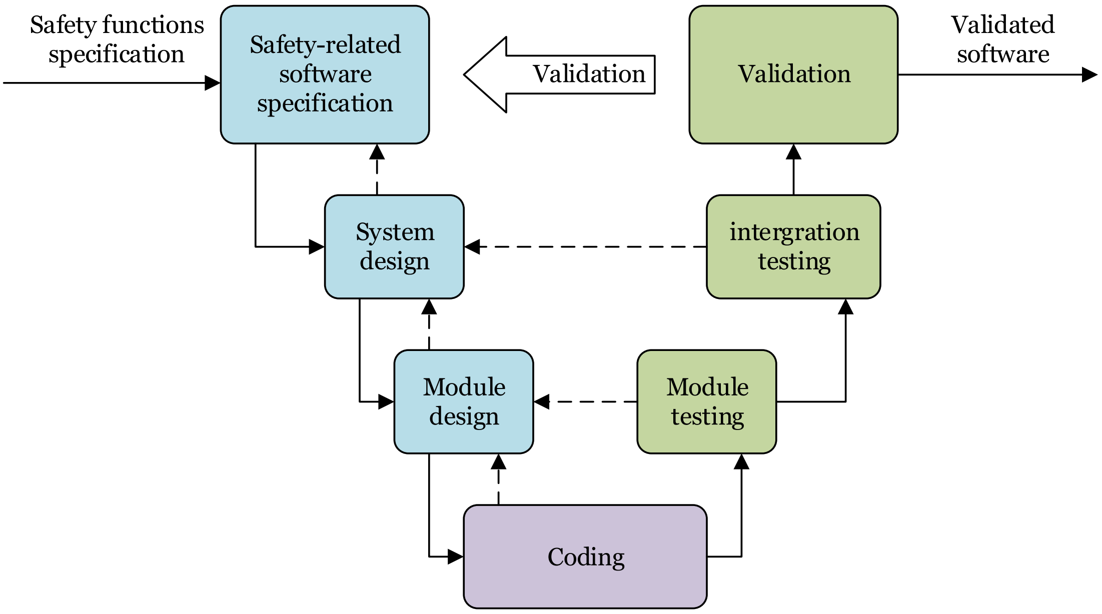


Figure 21 V-Model for software verification and validation

Legend:

The main goal of the V-model is to verify that the software, which is implemented in the logic-unit of a safety function fulfills the software requirements in EN ISO 13849-1:2016. The process starts with specifying the software specification requirements for each safety function and determine what shall be involved in the safety related software. Different aspects to consider for the safety-related software specification are:

- Performance criteria's
- Real time properties
- Operating modes
- Hardware architecture
- Self-Diagnostics

A system design can be formed from the safety-related software specification. The purpose of the system is to have a modular and structured software design. The system can be subdivided into modules which solves different tasks of the control system. Modules are a good way to separate different functions of the control system and to reduce the risk of faults, while ensuring that each module can be tested individually.

With a system design with modules, can the software developer start to write the actual code for every function of the system. It's required that the software developer uses a modular and structured programing strategy.

It's important to verify and validate every new function which has been developed that it fulfils the safety-related software specification. Therefore, should a software developer verify and validate each function continuously throughout the whole development prosses of the software.

In EN ISO 13849-1:2016, Annex J is a more detailed explanation of the software requirements presented together with programming rules.

7 Hardware architecture (allocation)

When realizing a product/application it's important to identify the safety related and non-safety related parts of the construction. In this section is the identification of safety related components discussed followed by discussion of allocation and realization of the safety function.

7.1 Identification

When identifying the SRP/CS which corresponds to parts of the safety function can Figure 22 be used as support. Sometimes it's easier to distinguishing which parts of the control system which are not safety related rather than trying to find the safety related.

In general:

- If a fault of any part of the control system increases the probability of occurrence of hazardous event, then that part shall be considered as a SRP/CS. While also be included in the safety function.
- A safety function may have several safety related inputs, while also having several safety related outputs. Safety functions may share components. Such as logic units or outputs to power control elements.
- Safety functions can be complex and have multiple SRP/CS in series connections.

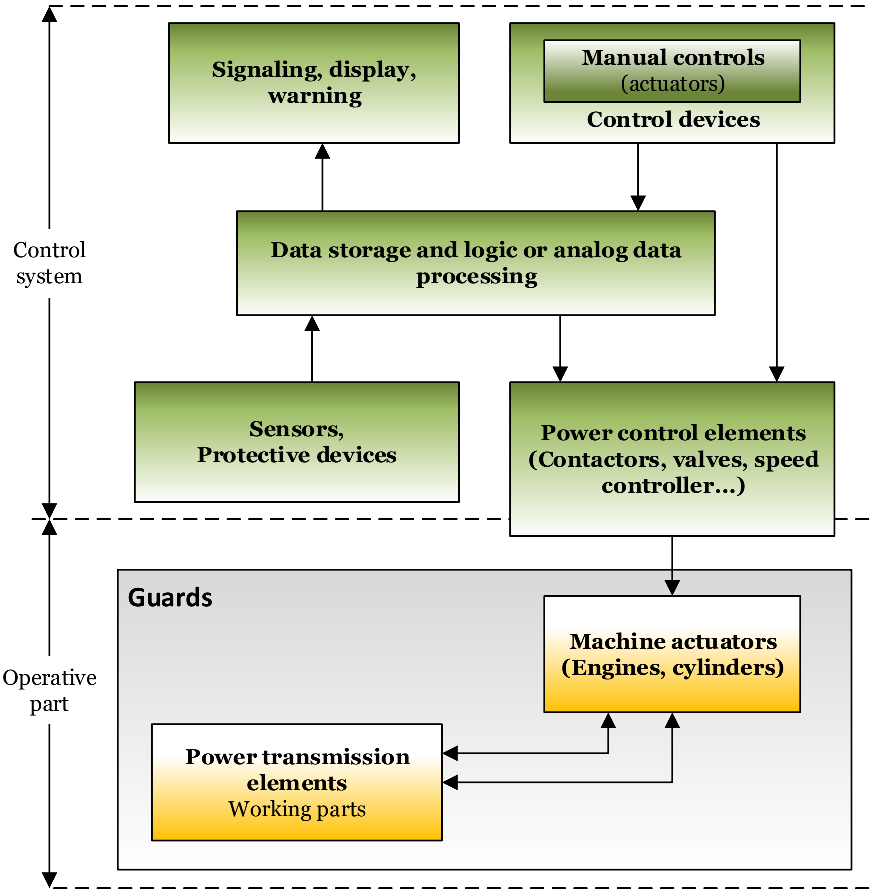

Signaling, display, warning
Manual controls
(actuators)
Control devices
Control system
Data storage and logic or analog data processing
Sensors, Protective devices
Power control elements (Contactors, valves, speed controller...)
Guards
Machine actuators (Engines, cylinders)
Operative part
Power transmission elements
Working parts

Figure 22 Overview of a control system with operative part

From the risk analysis of a product/application can different hazardous situations be highlighted. Some of these highlighted situations can be countered with inherent safe design and some situations can be countered with a safety function.

In the risk analysis is usually the hazardous situation presented with an event which can be used to identify the hazard. The initial event of the hazardous situation shall be used as input to the safety function.

The initial event is detected by the SRP/CS$_{\text{Input}}$ and sent to the logic unit for processing. Depending on the initial hazardous event can different safety related actions be executed by the safety function.

When allocating the safety function, it's important to find the components which corresponds to each part of the ILO-system. Starting with the initial event, where it's detected by the safety function, what components is responsible for detecting the hazardous event. This is the input part of the safety function, consisting of sensors, indicators or other measures to detect the dangerous event.

A signal is often sent to some logic device when a sensor has detected a hazardous event. The logic device is deciding an appropriate action depending on the hazardous event. A signal is sent from the output of the logic unit when an appropriate action has been decided. For example, can the output be the final power control elements, which is turning of the power to the main relays to a motor.

7.2 The PL_r decides the architecture

From the risk analysis is a required performance level for risk reduction stated. This performance level decides which designated architecture that can be chosen to realize the safety function. The first decision that needs to be consider when realizing a safety function is what designated architecture is necessary to achieve the required performance level.

7.2.1 Realizing a single channel safety function

For single channel safety functions are there two options of designated architecture available: Category B and 1. Depending on the required performance level of the safety function can either a category B or 1 be decided to be realized. The highest PL a single channel safety function can achieve is PL_c.

Category B and 1 architecture don't have any diagnostic coverage since there are no monitoring of faults of the safety function. So, the diagnostic coverage is always DC_{avg} = none.

The main difference between a category B and 1 architecture is the quality of the SRP/CS. Which decides the $MTTF_d$. For a category B architecture is only two possible options available, $MTTF_d$ = Low or Medium. Depending on the chosen components can a category B architecture achieve a PL of either a or b. However, for a category 1 architecture is always $MTTF_d$ = High due to the "well-tried" components and safety principles. Which means that a category 1 design is less likely to fail due to better quality of the SPR/CS.

It's necessary to evaluate that the decided designated architecture fulfils the risk reductive measure that was required for the safety function. Methods on how to evaluate characteristics of the SRP/CS are presented in section 3, while a method to estimate the achieved PL of the safety function is presented in section 8, in this report.

7.2.2 Realizing a safety function with monitoring

There are three different designated architectures available for safety functions with monitoring, namely category 2, 3 and 4. Depending on the required performance level of the safety function can either a category 2, 3 or 4 be decided to be realized. The highest achievable PL for safety functions with monitoring is PL_e.

Category 2, 3 and 4 safety function has monitoring of faults of the safety function which mean that the DC_{avg} can range between Low and Medium. For category 4 architectures is there only one option which is DC_{avg} = High.

The $MTTF_d$ for category 2 and 3 designs can range from Low to High, which corresponds to different achieved PL. While a category 4 safety function requires a $MTTF_d$ = high.

As in the case for single channel safety function it's important to evaluate the achieved risk reductive measure compared to what was required. Methods on how to evaluate characteristics of the SRP/CS are presented in section 3, while a method to estimate the achieved PL of the safety function is presented in section 8, in this report.

7.2.3 Difference between a category 2 and category 3

To be able to compare the two architectures it's necessary to first state what the two architectures have in common, before stating what the differences are. Both architectures have the following properties in common:

- Requirements of "well-tried" components and safety principles
- Monitoring of faults of the safety related components

The main differences between a category 2 and a category 3 designated architecture lies within the system behaviours in the event of faults of the safety function.

Both categories shall have fault monitoring by automatic online diagnostic tests. However different failures of the components/parts can have different effects depending on the category.

EN ISO 13849-1:2016 states that a component failure for a category 2 will only be detected when a self-check is performed. This means that there might take some time between the occurrence of the fault until it's detected and handled by the control system. This implies that the safety function might be lost in between checks. In the event of a detected fault of the safety function there is only one option for a category 2, which is to initialize the safe state (i.e. perform the safety function).

A category 3 shall whenever reasonably practical be able to detect and handle a single fault of the safety function. Furthermore, shall a single detected fault not lead to the loss of the safety function. This implies that a category 3 architecture can handle single faults and still be able to fulfil its risk reductive measure. This is fulfilled through the two redundant channels of the safety function. In the event of a failure of one channel of the safety function, shall the other channel still fulfil its risk reducing measure of the safety function.

One additional difference between a category 2 and 3 designated architecture is that a category 2 architecture only has one functional channel with monitoring while a category 3 has two redundant channels where both channels ensures that the safety function is working.

8 Achieved risk reduction

With a designated architecture and SRP/CS identified and the characteristics evaluated and estimated can the final achieved risk reduction of the safety function be estimated. This section covers achieved risk reduction in general, achieved risk reduction by one SRP/CS and last, achieved risk reduction by several SRP/CS connected in series.

8.1 Achieved performance level

The achieved PL of a SRP/CS and finally the corresponding PL of the whole safety function can be determined by evaluating the following aspects:

- The mean time to dangerous failure ($MTTF_d$) value for single components
- The diagnostic coverage (DC)
- The common cause failure (CCF)
- The design category of the safety function
- The behaviours of the safety function under fault condition(s)
- Safety related software
- Systematic failure
- The ability to perform a safety function under expected environmental conditions

These aspects can be sorted into two groups:

- Quantified aspects ($MTTF_d$, DC, CCF, structure)
- Non-Quantified aspects, behaviour of the safety function under fault conditions, safety-related software, systematic failure and environmental conditions.

EN ISO 13849-1:2016 gives examples of several different methods to estimate the achieved PL of the safety function such as: Markov modelling, generalized stochastic petri nets (GSPN), reliability block diagrams [see, e.g. IEC 61508]. In section 9.2 in this report will reliability block diagrams be presented.

8.1.1 Performance level of a safety function realized as one SRP/CS

It's necessary to determine the quantified aspects of a safety function when evaluating the achieved PL. Since different combinations of designated architectures, DC_{avg} and $MTTF_d$ (for each channel) corresponds to different achieved PL for the safety function.

EN ISO 13849-1:2016 provides a simplified model to estimate the achieved PL of a safety function which has been realized as one SRP/CS, se Figure 23. To be able to utilize the simplified model it's required that the safety function is realized in accordance to the designated architecture, presented in section 5, in this report.

As seen in Figure 23 can different levels of $MTTF_d$ ($MTTF_d$ = Low, $MTTF_d$ = medium or $MTTF_d$ = High) cover more than one PL. For cases where the $MTTF_d$ is close to the border to achieve a higher/lower PL, it's necessary to compare the achieved $MTTF_d$ to the $MTTF_d$ levels where the PL is altered from one level to another. The different $MTTF_d$ levels can be found in the standard EN ISO 13849-1:2016, Annex K.

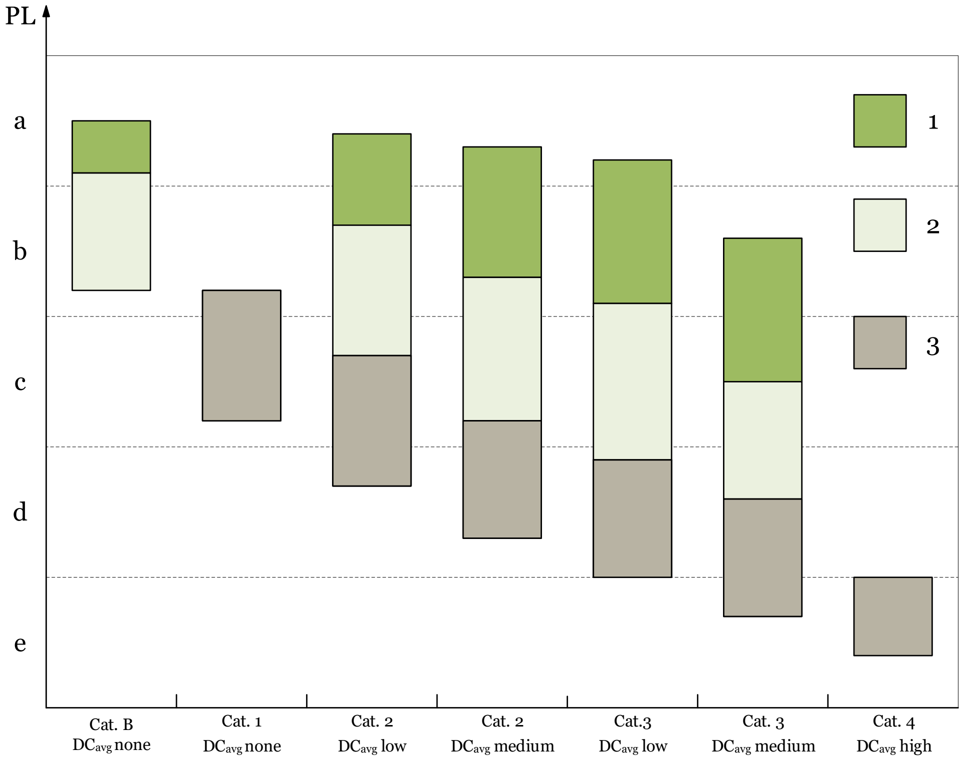


Figure 23 Achieved performance level depending on category, DC$_{avg}$ and MTTF$_d$ [EN ISO 13849-1:2016, Figure 5]

Legend:

PL	Performance level
1	MTTF$_d$ of each channel is low
2	MTTF$_d$ of each channel is medium
3	MTTF$_d$ of each channel is high
DC$_{avg}$	The average diagnostic coverage of the whole safety function

The designated architecture must be identified when evaluating the achieved PL of a safety function. In Table 7 below, are all designated architecture presented together with the channel representation of each category. In section 5 are the designated architecture and the properties of each category presented in detail. Measures against common cause failures must be implemented if the safety function is a dual-channel safety function.

Table 7 Channel representation of each designated architectures

Channel representation	
Design category	Channel representation
Category B	Single channel
Category 1	Single channel
Category 2	Single channel
Category 3	Double channel
Category 4	Double channel

When the designated architecture of the safety function has been identified the next step is to ensure that the requirements of diagnostic coverage are fulfilled. In section 4.2, in this report is diagnostics coverage presented in detail. In section 4.2.2 is a method of estimation of the average diagnostic coverage presented, which can be used to estimate the diagnostic coverage for ever SRP/CS of the safety function. Table 8 below presents the level of diagnostic coverage that a safety function can achieve.

Table 8 Diagnostic coverage [EN ISO 13849-1:2016, table 5]

DC	
Denotation	Range
None	$DC < 60\ \%$
Low	$60\ \% \leq DC < 90\ \%$
Medium	$90\ \% \leq DC < 99\ \%$
High	$99\% \leq DC$

With the designated architecture and the diagnostics coverage of the safety function identified shall the $\mathrm{MTTF_d}$ of the each SRP/CS be estimated. The $\mathrm{MTTF_d}$ is presented in detail in section 4.1 in this report together with methods to estimate the $\mathrm{MTTF_d}$ for different components. Each level of $\mathrm{MTTF_d}$ is also presented in Table 9 below.

Table 9 Levels of MTTFd [EN ISO 13849-1:2016, table 4]

$\mathrm{MTTF_d}$	
Denotation	Range
Low	$3\ years \leq MTTF_d < 10\ years$
Medium	$10\ years \leq MTTF_d < 30\ years$
High	$30\ years \leq MTTF_d \leq 100\ years$

8.1.2 Performance level of a safety function realized as several SRP/CS

With several SRP/CS in combination which shall fulfil a safety function can't Figure 23 be used to estimate the achieved performance level for the whole safety function. It's important to note that the PL of the individual SRP/CS can however be evaluated from Figure 23. EN ISO 13849-1:2016 only supports cascaded combination of SRP/CS, se Figure 24.

Typical examples of this is when:

- The safety function is a combination of SRP/CS which fulfils different designated architecture
- The safety function is realized by means of subsystems, COTS, see section 2.3

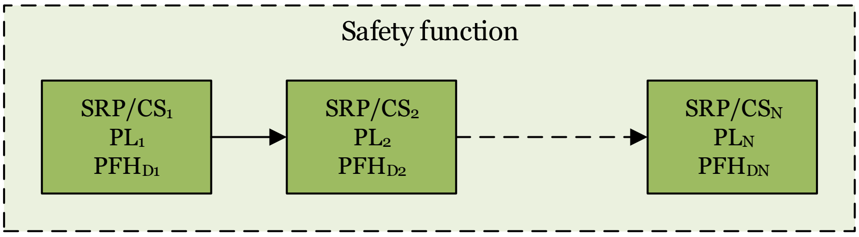

Safety function
SRP/CS$_1$ PL$_1$ PFH$_{D1}$
SRP/CS$_2$ PL$_2$ PFH$_{D2}$
SRP/CS$_N$ PL$_N$ PFH$_{DN}$

Figure 24 Cascaded SRP/CS which fulfils a safety function

Two approaches are available when estimating the achieved PL of the whole safety function.

First approach, the combined PFH$_d$ for each SRP/CS of the whole safety function can be sum up and used to evaluate the safety function, according to Figure 24. The PFH$_d$ can be found in the datasheets of the component or in EN ISO 13849-1:2016, Annex K if the designated architecture, DC$_{avg}$ and MTTF$_d$ is known for the SRP/CS. The total PFH$_d$ shall then be matched against the PL values from Annex K in the standard. The total achieved PFH$_d$ can be used together with Table 10 to match the PFH$_d$ to a PL.

A note to the method above is that the designated architecture of the individual SRP/CS has no impact on the achieved PL. It's only the PFH$_d$ which has an impact.

Table 10 Performance level (PL), PFH$_d$

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

Second approach, if the PFH_d is not known for the SRP/CS but the achieved PL is, then Table 11 can be used to evaluate the achieved PL for the whole safety function. This method can be more conservative and limits the amount of SRP/CS that may be combined.

The first step for this method is to identify the number of SRP/CS (N_{Low}), which has the lowest performance level (PL_{Low}). Then the table can be used to evaluate the achieved PL of the whole safety function.

Table 11 Series SRP/CS combination method [EN ISO 13849-1:2016, Table 11]

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

9 Hardware evaluation

When a safety function has been implementing/realizing, it's important to evaluate the chosen hardware. This can be done by a couple of different methods. In this section are Failure modes and effect analysis (FMEA) and Reliability Block Diagrams (RBD) presented as two different hardware analysis tools.

9.1 Failure modes and effect analysis

Failure modes and effect analysis is a systematic method to predict faults, evaluate the consequences and used to determine the correct fault measures. A FMEA evaluation can be performed on different levels of a product, for example the entire system, subsystems, assembly, subassembly or on part level. The process shall go through as many components, assemblies, subsystems as possible to detect failure modes and identify the corresponding consequences.

The product is first evaluated on a functional level until the product has developed enough to identify hardware components. The evaluation is then expanded to include these hardware components in evaluation as well. This process is then repeated throughout the entire design of the product, until a final product is presented.

A FMEA evaluation is usually performed by a group of different personnel working in different section of the product, a wide variety of personnel is desirable. Usually are personnel from design, assembling, operation and maintenance gathered to evaluate the product.

The results from a FMEA can be crucial during the development of a product. Since a FMEA can identify critical areas which needs to be changed to make the product safer. During the development of a product it's easier to make construction changes to the hardware in the early stages rather than towards end.

The findings from the evaluation is reported on a FMEA-spreadsheet where, each failure mode is presented together with relevant information. Information such as potential cause(s), local and global effects on the system, the probability of occurrence, severity, detection, risk level etc.

The probability of occurrence (P_d), severity (S) and detection (D), are estimated during the process and rated on a level from 1 to 10. For P_d is 1 to 10 an estimation of the occurrence of the fault, where 1 corresponds to a low probability of occurrence and 10 to a high level of occurrence. For S, 1 corresponds to no risk at all and 10 corresponds to fatality or amputation of limbs. While for D, 1 corresponds to the detection of the fault or the cause of the fault and 10 corresponds to an undetected fault.

These three properties of a failure mode are then combined and presented as a risk level (R). The risk level is calculated as $R = P_d * S * D$ where the result is a number ranging from 1 to 1000. It can be decided if the product requires different measures to reduce the risk level depending on the results of R.

9.2 Reliability block diagrams

Reliability block diagrams (RBD) is a systematic way to evaluate the reliability of a complex system by evaluating the failure rate Λ_D, of the components. RBD are usually visualized by an input, different blocks representing the components of the system and the final output. Each block is either connected in series or in parallel. Connections in parallel shows that a component is redundant.

The system will successfully work as long as there is at least one connection from input to output. RBD are often a representation of a physical components arranged by the schematics of the components.

Each system can either represent the whole system or it can represent subsystems which represent different parts of the whole system. Se Figure 25 for a representation of a RBD with both series and parallel connections.

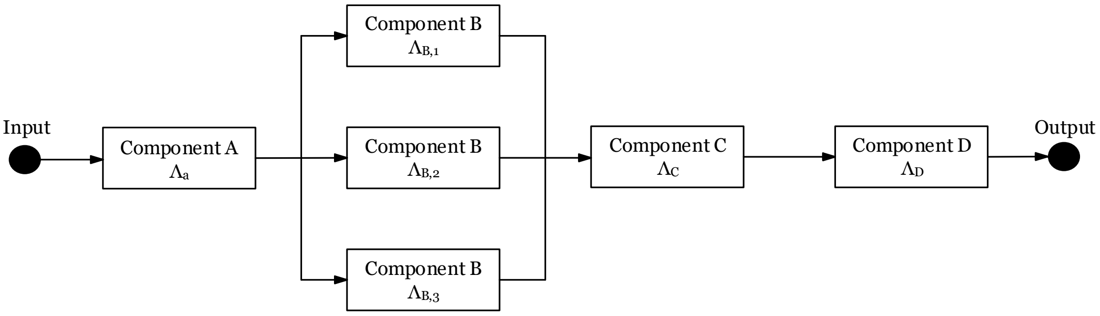


Figure 25 general RBD with both series and parallel connections

Complex components may also be divided into subsystems, since the component may have different failure modes, which have different failure rates. Se Figure 26 for a subsystem which contains three failure modes of component B.

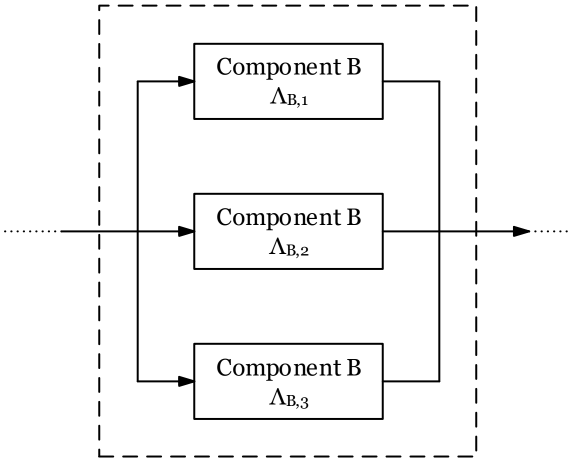


Figure 26 subsystem of a RBD

Appendix A Bibliography

A.1 Directive

Directive 2006/42/EC of the European Parliament and council on Machinery 17 May 2006 ("The EU Machinery Directive")

Download in many languages at
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006L0042

A.2 Standards

EN ISO 12100:2010 "Safety of machinery – General principles for design – risk assessment and risk reduction (ISO 1210:2010)"

EN ISO 13849-1:2016 "Safety of machinery – safety related parts of control systems – Part 1: General principles for design (ISO 13849-1:2016)"

ISO/TR 14121-2:2012 "Safety of machinery – Risk assessment – Part 2: Practical guidance and examples of methods (ISO 14121-2:2012, IDT)"

EN 61508:2010, part 1 "Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements (IEC 61508-1:2010)"

EN 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 (IEC 61508-2:2010)"

EN 61508:2010, part 4 "Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations (IEC 61508-4:2010)"

EN 574 +A1:2008, "Safety of machinery - Two-hand control devices - Functional aspects - Principles for design" (EN 574:1996+A1:2008)

EN 61496:2012, part 1 "Safety of machinery - Electro-sensitive protective equipment - Part 1: General requirements and tests" (IEC 61496-1:2012)

EN 61496:2016, part 3 "Safety of machinery - Electro-sensitive protective equipment - Part 3: Particular requirement for Active Opto-electronic Protective Devices responsive to Diffuse Reflection (AOPDDR)" (IEC 61496-3:2001)

Standards can be obtained from your standardisation body (e.g. http://www.sis.se/

Appendix B Abbreviations

B.1 Abbreviations table

Abbreviation:	Explanation:
Λ_D	Failure rate
Λ_d	Probability of total dangerous failures
Λ_{dd}	Probability of total detected dangerous failures
B_{10D}	Number of operations until 10% of the parts/components fail dangerously
c	Cross monitoring
CCF	Common Cause failures
COTS	Commercial of the shelf
D	Detection
DC	Diagnostic Coverage
DC_{avg}	Diagnostic Coverage Average
d_{op}	Mean operation, in days per year
EEA	Europa Economic Area
EU	European Union
F	Frequency and/or exposure to hazard
FIT	Failures in time
FMEA	Failure Mode and Effects Analysis
GSPN	Generalized Stochastic Petri Nets
h_{op}	Mean operation, in hours per day
I (I1, I2)	Input device, e.g. sensor
i_m	Interconnecting means
j	Component type

Abbreviation:	Explanation:
L	Logic device, e.g. processing unit
m	Monitoring
MTTF_d	Mean Time to Dangerous Failure
$\tilde{N}$	Number of different component types within the channel
n_j	Number of components of type *j* within the channel
N_{Low}	The number of identified SRP/CS
n_{op}	Mean number of operations
O (O1, O2)	Output device, e.g. main contactor
OTE	Output of TE
P	Probability of avoiding or limiting harm
P*d*	Probability of occurrence
PFH_d	Probability of Dangerous Failures per Hour [1/hour]
PL	Performance Level
PL_{Low}	Safety function with the lowest performance level
PL_r	Performance Level Required
R	Risk
RBD	Reliability Block Diagram
S	Severity of injury
SRASW	Safety-Related Application Software
SRESW	Safety-Related Embedded Software+
SRP/CS	Safety-related part of a control system
t_{cycle}	Mean operation time between the beginning of two successive cycles of the component.
TE	Test Equipment

Through our international collaboration programmes with academia, industry, and the public sector, we ensure the competitiveness of the Swedish business community on an international level and contribute to a sustainable society. Our 2,200 employees support and promote all manner of innovative processes, and our roughly 100 testbeds and demonstration facilities are instrumental in developing the future-proofing of products, technologies, and services. RISE Research Institutes of Sweden is fully owned by the Swedish state.

I internationell samverkan med akademi, näringsliv och offentlig sektor bidrar vi till ett konkurrenskraftigt näringsliv och ett hållbart samhälle. RISE 2 200 medarbetare driver och stöder alla typer av innovationsprocesser. Vi erbjuder ett 100-tal test- och demonstrationsmiljöer för framtidssäkra produkter, tekniker och tjänster. RISE Research Institutes of Sweden ägs av svenska staten.

RISE Research Institutes of Sweden AB
Box 857, SE-501 15 BORÅS, Sweden
Telephone: +46 10 516 50 00
E-mail: info@ri.se, Internet: www.ri.se

Electronics
RISE Report 2019:13
ISBN:978-91-88907-37-0