1- Introduction

The purpose of this section is to provide the machine manufacturer with a quick overview of a number of standards related to machine safety, to clarify some basic terms and to provide some application examples. This brief guide only covers aspects related to the functional safety of the machine, i.e., all measures that must be taken to protect the operating personnel from the hazards arising from the operation of the machine, as well as the project planning and selection of the appropriate interlocking devices for the given guard.
The machine designer himself must identify risks that are posed by other hazards, such as live parts, pressurised containers, explosive atmospheres, etc. These risks are not dealt with in this guideline.
Pizzato Elettrica prepared this document to the best of its knowledge, taking into consideration the standards, interpretations and existing technologies. The examples provided here must always be considered by the end customer with respect to the latest state of technology and standardisation. Pizzato Elettrica accepts no responsibility for the examples provided here and does not exclude the possibility of unintentional errors or inaccuracies.

2 -Design in safety. Structure of the European standards.

To freely market any type of device or machine in the countries of the European Community, they must comply with the provisions of the EU directives. They establish the general principles for ensuring that manufacturers place products on the market that are not hazardous to the operating personnel. The vast range of products pose many different hazards and, over time, has led to the release of various directives. As an example, consider the Low Voltage Directive 2014/35/EU, the Equipment for Explosive Atmospheres (ATEX) Directive 2014/34/EU, the Electromagnetic Compatibility Directive 2014/30/EU, etc. The hazards that arise from the operation of machinery are described in the Machinery Directive 2006/42/EC.
Conformity with the directives is certified by the Declaration of Conformity issued by the manufacturer and by the application of the CE marking on the machine.

For the assessment of risks posed by a machine and for the realisation of the safety systems for protecting the operating personnel from those risks, the European standardisation organisations CEN and CENELEC have issued a series of standards which translate the contents of the directives into technical requirements. The standards published in the Official Journal of the European Union are harmonised. The manufacturer is to verify conformity with the applied and listed standards.

The machine safety standards are divided into three types: A, B and C.
Type A standards: Standards that cover basic concepts and general principles for design in order to achieve safety in the design of machinery.
Type B standards: Standards that deal with one or more safety aspects and are divided into the following standards:
- B1: Standards on particular safety aspects (e.g. safety distances, temperature, noise, etc.)
- B2: Standards on safeguards (e.g. two-hand controls, interlocking devices, guards, etc.)

Type C standards: Standards that deal with detailed safety requirements for a particular group of machines (e.g. hydraulic presses, injection moulding machines, etc.)

The system or machine manufacturer must therefore determine whether the product is covered by a type C standard. If this is the case, this standard specifies the safety requirements; otherwise, the type B standards shall apply for any specific aspect or device of the product. In the absence of specifications, the manufacturer shall follow the general guidelines stated in the type A standards.

TYPE A STANDARDS
For example:

EN ISO 12100. Safety of machinery - General principles for design - Risk assessment and risk reduction.

TYPE B1 STANDARDS
For example:

EN 62061. Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems
EN ISO 13849-1 e -2. Safety-related parts of control systems

TYPE B2 STANDARDS
For example:

EN 574. Two-hand control devices
EN ISO 13850. Emergency stop
EN ISO 14119. Interlocking devices associated with guards
EN 60204-1. Electrical equipment of machines
EN 60947-5-1. Electromechanical control circuit devices

TYPE C STANDARDS
For example:

EN 201. Plastics and rubber machines - Injection moulding machines
EN 415-1. Safety of packaging machines
EN 692. Mechanical presses
EN 693. Hydraulic presses
EN 848-1. Safety of wood-working machines – One side moulding machines with rotating tool – Part 1: Single spindle vertical moulding machines

3 - Designing safe machines. Risk analysis.

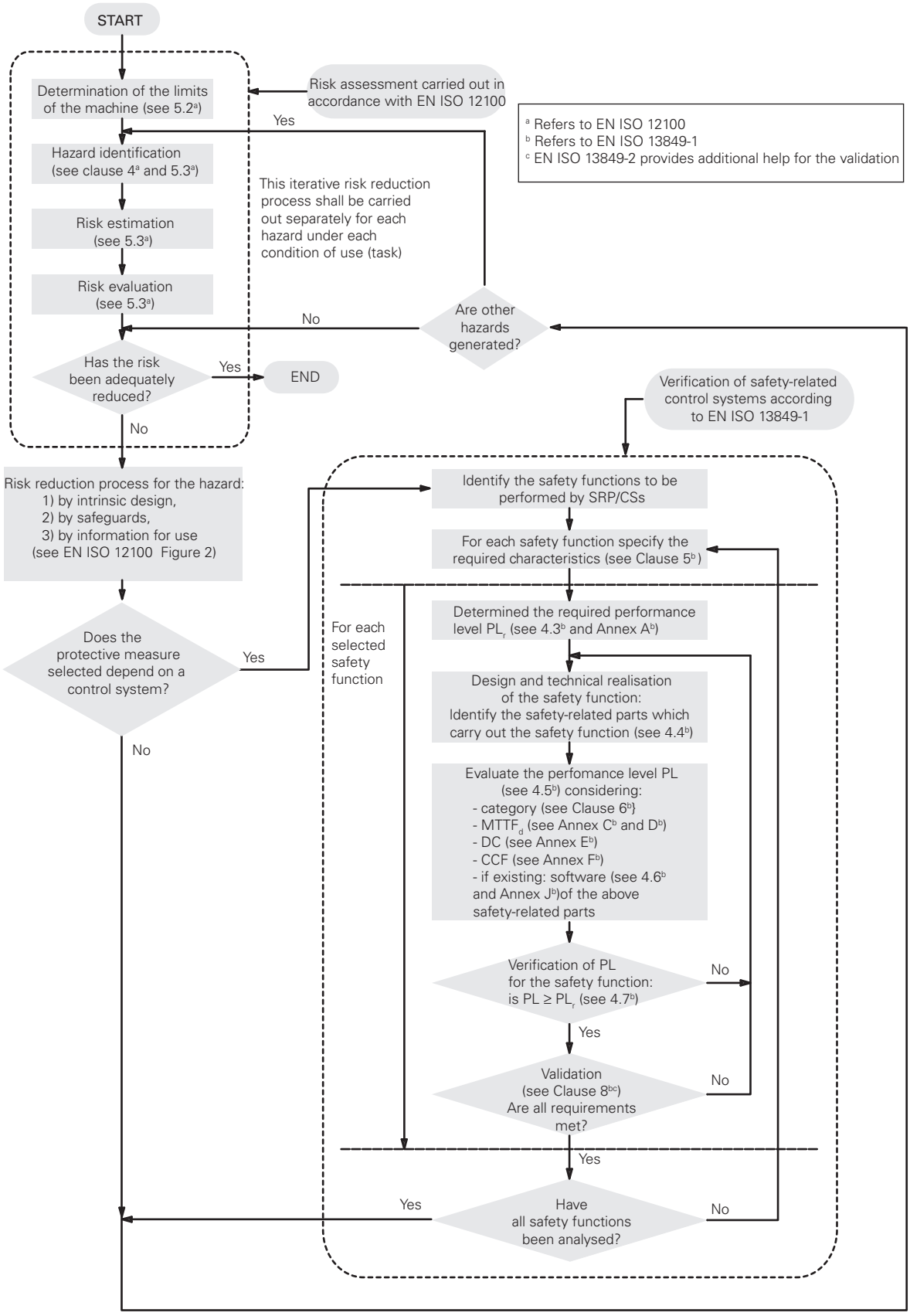
The first step in producing a safe machine is to identify the possible hazards to which the operators of a machine are exposed. The identification and classification of the hazards allows the risk for the operator or the combination of the probability of a hazard and the possible injury to be determined.

The methodology for risk analysis and evaluation and the procedure for the elimination/reduction of risks is defined by standard EN ISO 12100. This standard introduces a cyclic analysis model: starting with the initial objectives, the risk analysis and the various possibilities for reducing these risks are repeatedly evaluated until the initial objective is met.

The model introduced in this standard specifies that one proceed as follows after performing a risk analysis to reduce or eliminate risks:
1) Elimination of risks at their source through the use of intrinsically safe design principles and the structural set-up of the systems;
2) Risk reduction through safeguarding and monitoring systems;
3) Identification of residual risks though signalling and by informing the operating personnel.

Since every machine has hazards and because it is not possible to eliminate all possible risks, the objective is to reduce the residual risks to an acceptable level.

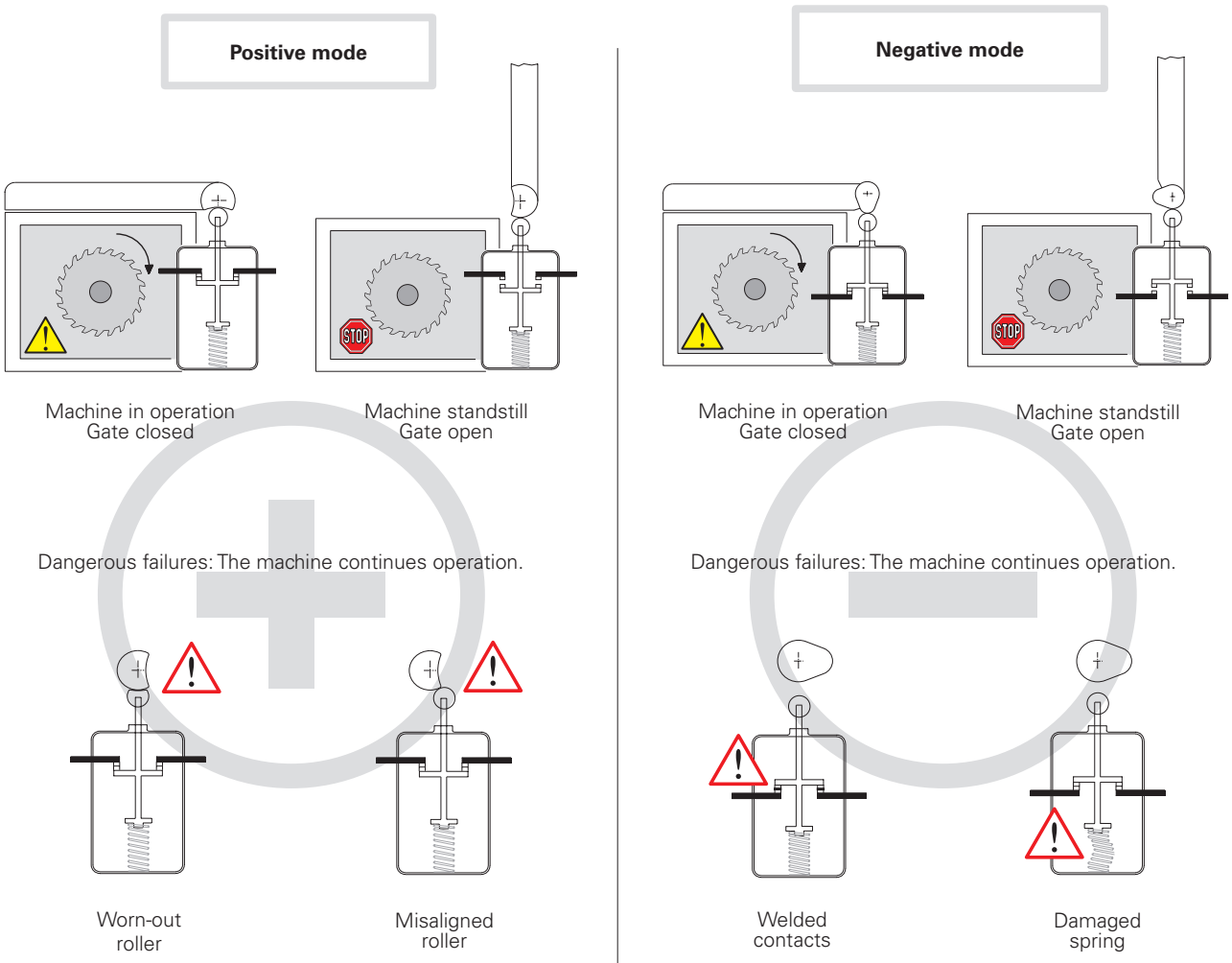
If a risk is reduced by means of a monitoring system, standard EN ISO 13849-1, which provides an evaluation model for the quality of this system, comes into play. If a given level is specified for a risk, it is possible to use a safety function of equal or higher level.



Note: This diagram was created by combining figures 1 and 3 of standard EN 13849-1. The texts in the diagram are not identical to those in the standard.

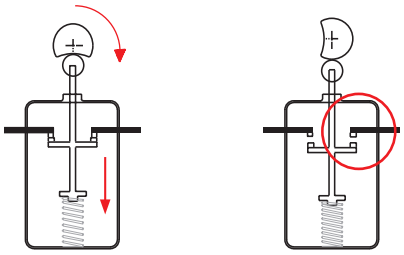
4 - Positive opening, redundancy, diversification and self-monitoring

Positive mode and negative mode.
According to the standard EN ISO 12100, if a moving mechanical component inevitably moves another component along with it, either by direct contact or via rigid elements, these components are said to be connected in the **positive** mode. Instead, if the movement of a mechanical component simply allows another element to move freely, without using direct force (for example by gravity force, spring effect, etc.), that connection is said to be connected in the **negative** mode.



With positive mode, preventive maintenance can be performed, thereby avoiding the dangerous failures described above. With negative mode, on the other hand, failures can occur within the switch and are therefore difficult to detect.
In the event of an internal failure (welded contacts or a damaged spring), the contacts will still open in positive mode in spite of the damage and the machine will be stopped.

Use of switches in safety applications
If only one switch is used in a safety application, the switch must be actuated in positive mode. In order to be used for safety applications, the opening contact (normally closed) must be with "**positive opening**". All switches with the symbol ⊖ are provided with NC contacts with positive opening.



No flexible connection between the moving contacts and the actuator on which the actuating force is exerted.

In case of two or more switches, they should operate in opposite modes, for example:
- The first with an NC contact (normally closed contact), actuated by the guard in positive mode.
- The other with an NO contact (normally open contact), actuated by the guard in negative mode.
This is a common practice, though it does not exclude the possible use of two switches that are actuated in positive mode (see diversification).

Diversification
In redundant systems, safety is increased through **diversification**. This can be obtained by using two switches with different design and/or technology; failures with the same cause can thereby be prevented. Examples for diversification include: the use of one switch with positive actuation and one switch without positive actuation, the use of one switch with mechanical actuation and one switch without mechanical actuation (e.g., electronic sensor) or the use of two switches with mechanical, positive actuation but with different types of actuation (e.g., an FR 693-M2 key switch and a switch with FR 1896-M2 hinge pin).

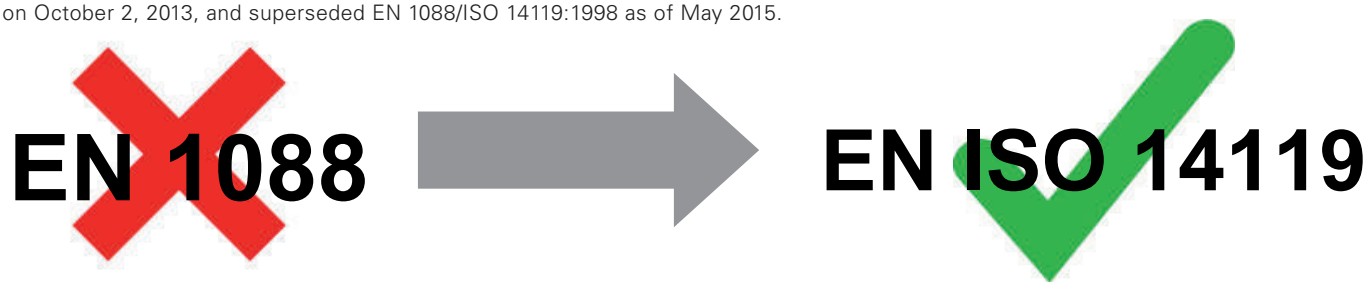
Redundancy
Redundancy implies the use of more than one device or system to make sure that, in case of a failure in one device, there is another one available to perform the required safety functions. If the first failure is not detected, an additional failure may lead to the loss of the safety function.

Self-monitoring
Self-monitoring consists in an automatic control performed to check the functioning of all devices involved in the machine working-cycle. This way the next working cycle can be either accepted or rejected.

Redundancy and self-monitoring
Combining **redundancy** and **self-monitoring** in the same system makes sure that a first failure in the safety circuit does not lead to the loss of safety functions. This first failure will be detected at the next re-start or, in any case, before a second failure which may lead to the loss of the safety function.

5 - Design and selection of interlocking devices associated with guards (standard EN ISO 14119)

The European standard EN ISO 14119 "Interlocking devices associated with guards – Principles for design and selection" came into force on October 2, 2013, and superseded EN 1088/ISO 14119:1998 as of May 2015.



The standard is intended for manufacturers of interlocking devices as well as machine manufacturers (and integrators) and describes the requirements on the devices and their correct installation.
The new standard provides clarification to a number of questions that are not always clear cut and considers the latest technologies used in the design of interlocking devices, defines a number of parameters (actuator type and level of coding) and describes the procedure for correct installation with the goal of minimizing the defeat possibilities of the interlocking devices.
The standard also considers other aspects related to interlocking devices (e.g. guard locking principles, electromagnetic guard locking, auxiliary release, escape and emergency release, etc.) which are not described here.

Coding level of the actuators

An important new addition to the standard is the definition of a coded actuator and the classification of the coding levels:
- **coded actuator** – actuator which was specially designed for use with a specific interlocking device;
- **low level coded actuator** – coded actuator for which 1 to 9 variations in code are available (e.g. the SR magnetic switch series or the safety switches with separate actuator and mechanical detection FS, FG, FR, FD…);
- **medium level coded actuator** – coded actuator for which 10 to 1000 variations in code are available;
- **high level coded actuator** – coded actuator for which more than 1000 variations are available. (e.g. the ST series sensors with RFID technology or the interlocking devices of the NG and NS series with RFID technology and guard locking).

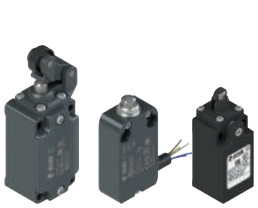
Types of interlocking devices

Standard EN ISO 14119 defines different types of interlocking devices:
- **Type 1 interlocking device** – interlocking device that is mechanically actuated by an uncoded actuator (e.g. HP series hinged interlocking devices)
- **Type 2 interlocking device** – interlocking device that is mechanically actuated by a coded actuator (e.g. safety switches with separate actuator of the FR, FS, FG, … series)
- **Type 3 interlocking device** – interlocking device that is contactlessly actuated by an uncoded actuator
- **Type 4 interlocking device** – interlocking device that is contactlessly actuated by a coded actuator (e.g. ST series safety sensors with RFID technology and NG and NS series safety switches with RFID technology)

Examples of actuation principles		Actuator examples		Type
Mechanical	Direct contact/force	Uncoded	Rotary cam	Type 1
			Linear cam	
			Hinge	
		Coded	Key-actuated	Type 2
			Trapped key	
Non-contact	Inductive	Uncoded	Ferromagnetic material	Type 3
	Magnetic		Magnet, solenoid	
	Capacitive		Any suitable object	
	Ultrasonic		Any suitable object	
	Optic		Any suitable object	
	Magnetic	Coded	Coded magnet	Type 4
	RFID		Coded RFID tag	
	Optic		Optically coded tag	

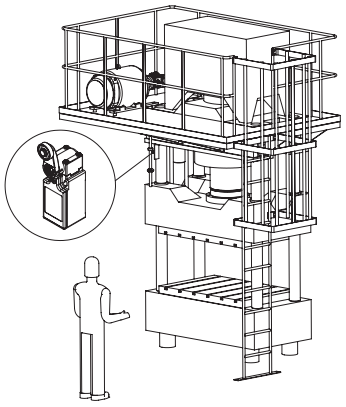
Excerpt from EN ISO 14119 - Table 1

Requirements for the design and the installation of interlocking devices according to EN ISO 14119 to reduce defeating of guards.

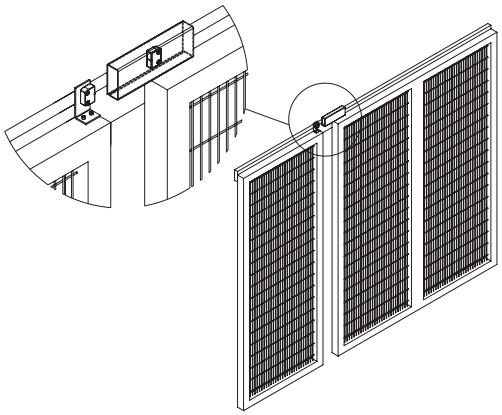
Principles and measures against defeating	Type 1 devices		Type 2 and type 4 devices	Type 2 and type 4 devices
	Cam safety switches rotary or linear cam	Safety hinge switches	Low and medium level coded actuators	High level coded actuators
				
Installation out of reach (1)	X		X	
Barriers or shielding (2)				
Installation in hidden position (3)				
Testing by means of control circuit (4)				
Non-detachable fixing of position switch and cam				
Non-detachable fixing of position switch		M		
Non-detachable fixing of the actuation element or cam		M	M	M
Additional position sensing and plausibility check	R		R	

Excerpt from EN ISO 14119 - Table 3

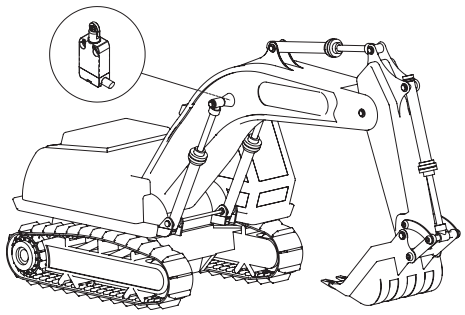
X: mandatory to apply at least one of the measures listed in the "Principles and measures" column
M: mandatory measure
R: recommended measure
It is clear that the use of devices with RFID technology, high coding level and hinged switches is the easiest way to meet the requirements of EN ISO 14119, as it is only necessary to fulfil a few requirements in order to prevent defeating of guards.
Devices with low or medium coding level require additional measures to ensure a tamperproof application.



(1) - Installation out of reach



(2) - Barriers or shielding



(3) - Installation in hidden position

(4) - Status monitoring or periodic testing can, for example, be performed on a machine with a simple operating cycle so as to verify that the guards are actually open at the end of or during specific operating phases (e.g. to remove the processed material or to perform quality controls). If status monitoring does not detect opening of the guard, an alarm is generated and the machine is stopped.

Guard locking devices and holding force

The manufacturer of the interlocking device with guard locking must ensure that the device can withstand at least the measured holding force F_{Zh} while the interlock is engaged. This holding force must not exceed the maximum holding force divided by a safety coefficient equal to 1.3.
Example: A device with maximum holding force of F_{Zh} =2000 N must pass a test with a maximum holding force equal to F_{1max} =2600 N.
An interlocking device with guard locking can both monitor the position of the guard (open/closed) as well as lock the guard (locked/unlocked). Each of the two functions may require a different PL safety level (acc. to EN ISO 13849-1). The guard locking function generally requires a lower PL than the position monitoring function. (See paragraph 8.4, note 2 of EN ISO 14119).
To identify whether an interlocking device also performs status monitoring, the standard specifies that the product label includes the symbol shown to the side here.

$$F_{Zh} = \frac{F_{1max}}{1{,}3}$$

6 - Current status of the standards. Reason for changes, new standards and some overlapping

The "traditional" standards for functional safety, such as EN 954-1, played a large part in formalising some of the basic principles for the analysis of safety circuits on the basis of deterministic principles. On the other hand, they make no mention of the topic of programmable electronic control systems and are not generally in line with the current state of technology. To take programmable electronic control systems into account in the analysis of safety circuits, the approach taken by current standards is fundamentally probabilistic and introduces new statistical variables.

This approach is based on IEC 61508, which deals with the safety of complex programmable electronic systems and is very extensive (divided into 8 sections with nearly 500 pages). It is also used in a diverse range of application fields (chemical industry, machine construction, nuclear plants). This standard introduces the SIL concept (Safety Integrity Level), a probabilistic indication of a system's residual risk.

From IEC 61508 comes EN 62061, which covers the functional safety of the complex electronic or programmable control systems in industrial applications. The concepts introduced here permit general use for any safety-related electrical, electronic and programmable electronic control systems (systems with non-electrical technologies are not covered).

EN ISO 13849-1, developed by CEN under the aegis of ISO, is also based on this probabilistic approach. This standard, however, attempts to structure the transition to the concepts in a less problematic way for the manufacturer, who is accustomed to the concepts of EN 954-1. The standard covers electromechanical, hydraulic, "non-complex" electronic systems and some programmable electronic systems with predefined structures. EN ISO 13849-1 is a type B1 standard and introduces the PL concept (Performance Level); as with SIL, the concept provides a probabilistic indication of a machine's residual risk. This standard points out a correlation between SIL and PL; concepts borrowed by EN 61508 – such as DC and CCF – are used and a connection to the safety categories of EN 954-1 is established.

Important note
EN 13849-1 is a type B1 standard; if a type C standard is already applied for a machine, the type C standard is to be used. Some type C standards not yet updated are based on the concepts of EN 954-1. For manufacturers of machines that are covered by a type C standard, the introduction time of the new standards depends on how quickly the various technical committees update the C standards.

In the area of functional safety for the safety of control circuits, there are thus two standards presently in force:
EN ISO 13849-1. Standard type B1, which uses the PL concept.
EN 62061. Standard type B1, which uses the SIL concept.

There is clear overlapping of the two standards EN 62061 and EN ISO 13849-1 concerning their application field and many aspects are similar; there is also a link between the two symbol names (SIL and PL), which indicate the result of the analyses according to the two standards.

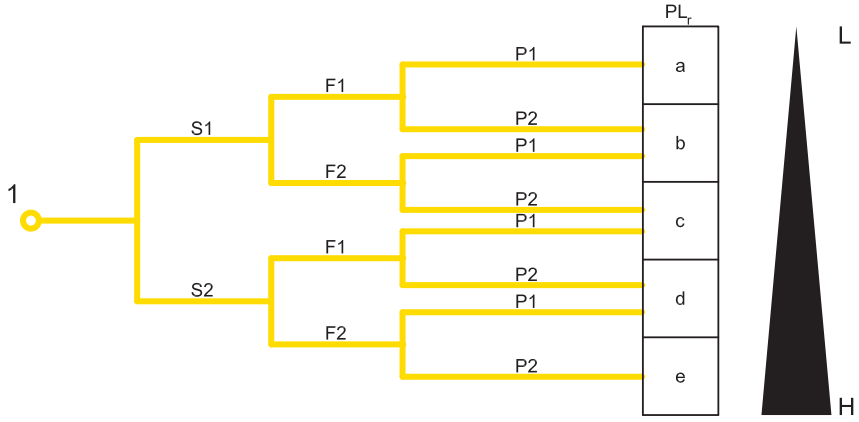
PL EN ISO 13849-1	**a**	**b**	**c**	**d**	**e**
SIL EN 62061 - IEC 61508	**-**	**1**	**1**	**2**	**3**
PFH_D	from 10^{-4} to 10^{-5}	from 10^{-5} to $3x10^{-6}$	from $3x10^{-6}$ to 10^{-6}	from 10^{-6} to 10^{-7}	from 10^{-7} to 10^{-8}
A hazardous failure every n years	from ~1 to ~10	from ~10 to ~40	from ~40 to ~100	from ~100 to ~1000	from ~1000 to ~10000

The choice of the standard to be applied is left to the manufacturer according to the technology that is used. We believe that standard EN ISO 13849-1 is easier to use thanks to its mediatory approach and the re-utilisation of the concepts already introduced on the market.

7 - Standard EN ISO 13849-1 and the new parameters: PL, $MTTF_D$, DC, CCF

Standard EN ISO 13849-1 offers the manufacturer an iterative method for assessing whether the hazards posed by a machine can be reduced to an acceptable residual level through the use of appropriate safety functions. The applied method specifies a hypothesis-analysis-validation cycle for each risk. Once completed, it must be possible to demonstrate that every selected safety function is appropriate for the respective risk.
The first step involves the determination of the required performance level, which is required of each safety function. Like EN 954-1, EN ISO 13849-1 also uses a risk graph for the risk analysis of a machine function (figure A.1). Instead of a safety category, however, this graph is used to determine – as a function of the risk – a Required Performance Level or PL_r for the safety function which protects the respective part of the machine.
Starting with point 1 of the graph, the machine manufacturer answers questions S, F and P and can then determine the PL_r for the safety function being examined. He must then develop a system with a performance level PL that is equal to or greater than that which is required to protect the operating personnel.

Risk graph for determining the required PL_r for the safety function (excerpt from EN ISO 13849-1, figure A.1)



Key

1 Starting point for the evaluation of the safety function's contribution to risk reduction
L Low contribution to risk reduction
H High contribution to risk reduction
PL_r Required performance level

* F1 should be selected if the total duration of the exposure to the hazard does not exceed 1/20 of the total work time and the frequency of exposure to the hazard does not exceed once every 15 minutes
****** If there are no other reasons, F2 should be selected if the frequency of exposure to the hazard is greater than once every 15 minutes.

Risk parameters

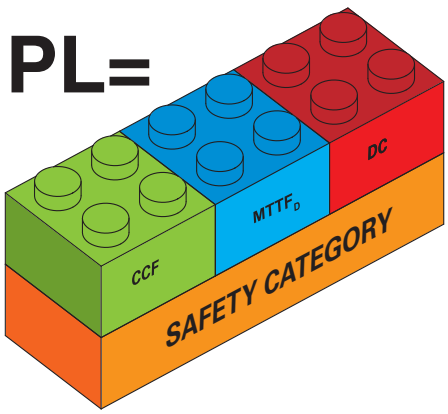
S Severity of injury
S1 Slight (normally reversible injury)
S2 Serious (normally irreversible injury or death)
F Frequency and/or exposure to hazard
***F1** Seldom-to-less-often and/or exposure time is short
****F2** Frequent-to-continuous and/or exposure time is long
P Possibility of avoiding hazard or limiting harm
P1 Possible under certain conditions
P2 Scarcely possible

Note: For a machine manufacturer, it may be of interest forego repeating the risk analysis of the machine and to instead to try and reuse the data already derived from the EN 954-1 risk analysis.
This is not generally possible, since the risk graph changed with the new standard (see previous figure) and, as a result, the required performance level of the safety function may have changed with identical risks. The German Institute for Occupational Safety and Health (BGIA), in its report 2008/2 on EN ISO 13849-1, recommends the following: assuming the "worst case", implementation can occur according to the table to the right. For further information, refer to the mentioned report.

Category required by EN 954-1		Required performance level (PLr) and category acc. to EN ISO 13849-1
B	→	b
1	→	c
2	→	d, Category 2
3	→	d, Category 3
4	→	e, Category 4

There are five performance levels, from PL a to PL e, with increasing risk; each represents a numerical range for the average probability of a dangerous failure per hour. For example, PL d specifies that the average probability of dangerous failures per hour is between $1x10^{-6}$ and $1x10^{-7}$, i.e., about 1 dangerous failure every 100-1000 years.

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

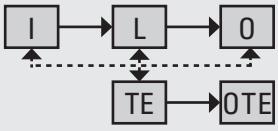
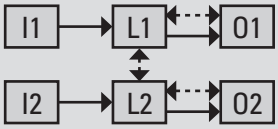
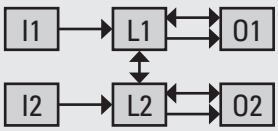


Several parameters are needed to determine the PL of a control system:
1. The safety category of the system, which is dependent on the architecture (structure) of the control system and its behaviour in the event of damage
2. $MTTF_D$ of the components
3. DC or Diagnostic Coverage of the system.
4. CCF or Common Cause Failures.

Safety category.
Most control circuits normally used can be represented with the following logic components:
- Input or signal input
- Logic or signal processing logic
- Output or output of the monitoring signal

These are connected to one another differently depending on the structure of the control circuit.

EN ISO 13849-1 allows for five different basic circuit structures, referred to as the designated architectures of the system. As shown in the following table, the architectures – combined with the requirements on the system behaviour in the event of failure and the minimum values of $MTTF_D$, DC and CCF – give the safety category of the system control. Thus, the safety categories of EN ISO 13849-1 are not the equivalent, but rather extend the concept of the safety category introduced by the previous standard EN 954-1.

Category	Summary of the requirements	System behaviour	Safety principles	$MTTF_D$ of each channel	DC_{avg}	CCF
B	Safety-related parts of monitoring systems and/or their protective equipment, as well as their accessories, must be designed, constructed, selected, assembled and combined in accordance with the relevant standards so that they can withstand the expected influences. Fundamental safety principles must be used. Architecture: 	The occurrence of a fault can lead to the loss of the safety function.	Mainly determined by the selection of components	Low to medium	None	Not relevant
1	In addition to the requirements of Category B, proven components and safety principles must be used. Architecture: 	The occurrence of a fault can lead to the loss of the safety function; the probability of fault occurrence is, however, lower than for Category B.	Mainly determined by the selection of components	High	None	Not relevant
2	Requirements of Category B and proven safety principles must be used. The safety function must be checked at appropriate intervals by the control system. Architecture: 	The occurrence of a fault between two checks can lead to the loss of the safety function. The loss of the safety function is detected through the check.	Determined mainly by the structure	Low to high	Low to medium	See Annex F
3	Requirements of Category B and proven safety principles must be used. Important safety-related parts must be designed so that: - A single fault in any of these parts does not lead to the loss of the safety function. - Where reasonably practicable, the single fault is detected. Architecture: 	If a single fault occurs, the safety function is always performed. Some, but not all faults are detected. Accumulation of undetected faults can lead to the loss of the safety function.	Determined mainly by the structure	Low to high	Low to medium	See Annex F
4	Requirements of Category B and proven safety principles must be used. Important safety-related parts must be designed, so that: - a single fault in any of these parts does not lead to the loss of the safety function, and - a single fault during or before the next request for the safety function is detected. If this is not possible, the accumulation of undetected faults must not lead to the loss of the safety function. Architecture: 	If a single fault occurs, the safety function is always performed. The detection of accumulated faults reduces the probability of the loss of the safety function (high DC). The faults are detected in time to prevent the loss of the safety function.	Determined mainly by the structure	High	High (including accumulation of faults)	See Annex F

$MTTF_D$ ("Mean Time To Dangerous Failure").
This parameter is used to determine the functional system quality over the mean lifetime in years before a dangerous failure occurs (other failures are not considered). The calculation of the $MTTF_D$ is based on numerical values supplied by the manufacturers of the individual components of the system. In the absence of this data, the values can be taken from the tables with guide values included in the standard (EN ISO 13849-1 Annex C). The evaluation results in a numerical value, divided into three categories: High, Medium or Low.

Classification	Values
Not acceptable	$MTTF_D$ < 3 years
Low	3 years ≤ $MTTF_D$< 10 years
Medium	10 years ≤ $MTTF_D$< 30 years
High	(30 years ≤ $MTTF_D$ ≤ 100 years

For components that are susceptible to high wear (typical for mechanical and hydraulic devices), the manufacturer supplies the value B_{10D} for the component, i.e., the number of component operations within which 10% of the samples failed dangerously, instead of the $MTTF_D$ of the component.
The B_{10D} value of the component must be converted to $MTTF_D$ by the machine manufacturer using the following formula:

$$MTTF_D = \frac{B_{10_D}}{0{,}1 \cdot n_{op}}$$

Where n_{op}= means number of annual operations for the component.
By assuming the daily operating frequency and the daily operating hours for the machine, n_{op} can be calculated as follows:

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3600s/h}{t_{ciclo}}$$

where
d_{op}= work days per year
h_{op}= operating hours per day
t_{cycle}= cycle time (s)

For components that are susceptible to wear, note that parameter $MTTF_D$ is dependent not only on the component itself but also on the application. An electromechanical device with low frequency of use, e.g. a remote switch that is only used for emergency stops, has a high $MTTF_D$; if the same device is used for normal processes in the operating cycle, the $MTTF_D$ of the same remote switch could drop dramatically.

All elements of the circuit contribute to the calculation of the $MTTF_D$ depending on their structure. In control systems with single-channel architecture (as is the case in categories B, 1 and 2), the contribution of each components is linear and the $MTTF_D$ of the channel is calculated as follows:

$$\frac{1}{MTTF_D} = \sum_{i=1}^{N} \frac{1}{MTTF_{D\,i}}$$

To avoid overly optimistic designs, the maximum value of the $MTTF_D$ of each channel is limited to 100 years (for categories B, 1, 2 and 3) or 2500 years (category 4). Channels with an $MTTF_D$ of less than 3 years are not allowed.

For two-channel systems (categories 3 and 4), the $MTTF_D$ of the circuit is calculated by averaging the $MTTF_D$ of the two channels using the following formula:

$$MTTF_D = \frac{2}{3}\left[MTTF_{DC1} + MTTF_{DC2} - \frac{1}{\frac{1}{MTTF_{DC1}} + \frac{1}{MTTF_{DC2}}}\right]$$

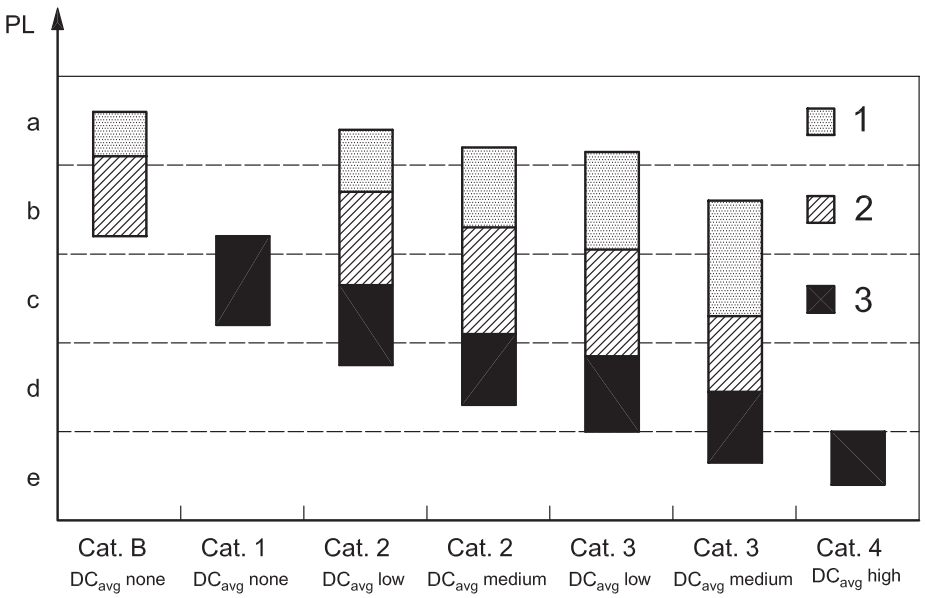
DC ("Diagnostic Coverage").

This parameter provides information on the effectiveness of a system's ability to self-detect any possible failures within the system. Using the percentage of the detectable dangerous failures, one obtains a diagnostic coverage of better or worse quality. The numerical DC parameter is a percentage value which is calculated using values taken from a table (EN ISO 13849-1 Annex E). Depending on the measures for failure detection taken by the manufacturer, example values are provided there. Because multiple measures are normally taken to rectify different anomalies in the same circuit, an average value or a DC_{avg} is calculated and can be assigned four levels:
High $DC_{avg} \geq 99\%$
Medium $90\% \leq DC_{avg} < 99\%$
Low $60\% \leq DC_{avg} < 90\%$
None $DC_{avg} < 60\%$
A diagnostic coverage of none is only permissible for systems of category B or 1.

CCF ("Common Cause Failures")
For the calculation of the PL for systems of category 2, 3 or 4, it is also necessary to evaluate possible common cause failures or CCF, which may compromise the redundancy of the system. The evaluation is performed using a checklist (Annex F of EN ISO 13849-1); on the basis of the measures taken against common cause failures, points from 0 to 100 are assigned. The minimum permissible value for categories 2, 3 and 4 is 65 points.

PL ("Performance Level")
After determining this data, EN ISO 13849-1 gives the PL of the system using an assignment table (EN ISO 13849-1) or, alternatively, using a simplified graphic (EN ISO 13849-1, paragraph 4.5) as shown in the following.

Relationships between the categories, DC_{avg}, $MTTF_D$ of each channel and PL (acc. to EN ISO 13849-1, figure 5)



1 = $MTTFD_{of\ each\ channel\ =\ Low}$ (3 years ≤ $MTTF_D$ < 10 years)

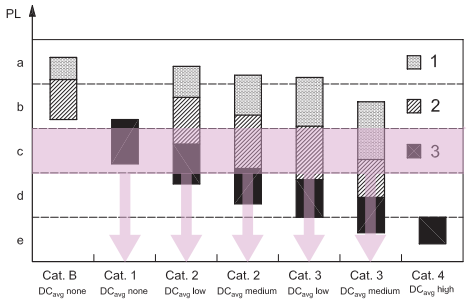
2 = $MTTF_D$ of each channel = Medium (10 years ≤ $MTTF_D$ < 30 years)

3 = $MTTF_D$ of each channel = High (30 years ≤ $MTTF_D$ ≤ 100 years)

This figure is very useful, as it can be read from multiple points of view. For a given PL_r, it shows all possible solutions with which this PL can be achieved, i.e., the possible circuit structures that provide the same PL.

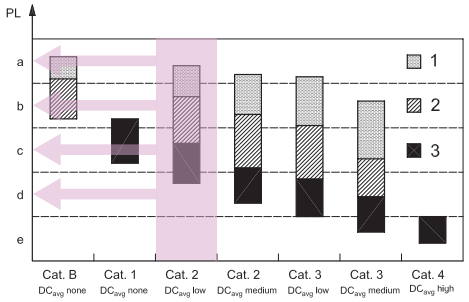
Considering the figure more closely, it is seen that the following possibilities exist for a system with PL equal to "c":

1. Category 3 system with less reliable components ($MTTF_D$=low) and medium DC.
2. Category 3 system with reliable components ($MTTF_D$=medium) and low DC.
3. Category 2 system with reliable components ($MTTF_D$=medium) and medium DC.
4. Category 2 system with reliable components ($MTTF_D$=medium) and low DC.
5. Category 1 system with very reliable components ($MTTF_D$=high).



Considering a given circuit structure, in this figure one can also identify the maximum PL that can be reached depending on the average diagnostic coverage and the $MTTF_D$ of the components.
Thus, the manufacturer can exclude a number of circuit structures in advance, as they do not meet the required PL_r.

However, the figure is not usually used to determine the PL of the system since the graphic areas overlap the boundaries of the different PL levels in many cases. Instead, the table in Annex K of standard EN ISO 13849-1 is used to precisely determine the PL of the circuit.



Notes

Table of safety parameters

The B_{10D} data in the table refers to the mechanical life of the device contacts under normal ambient conditions.
The value of B_{10D} for NC and NO contacts refers to a maximum electrical load of 10% of the current value specified in the utilisation category. Mission time (for all articles listed below): 20 years.

Electromechanical control devices

Series	Article description	B_{10D} (NO)	B_{10D} (NC)	B_{10}/B_{10D}
F• ••••	Position switches	1,000,000	40,000,000	50%
F• ••93 F• ••92	Safety switches with separate actuator	1,000,000	2,000,000	50%
F• ••99 F• ••R2	Safety switches with separate actuator with lock	1,000,000	1,000,000	50%
FG	Safety switches with separate actuator with lock	1,000,000	5,000,000	20%
FS	Safety switches with separate actuator with lock	1,000,000	4,000,000	20%
F• ••96 F• ••95	Safety switches with hinge pin	1,000,000	5,000,000	20%
F• ••C•	Switches with slotted hole lever for hinged guards	1,000,000	2,000,000	50%
F• ••••	Rope switches for emergency stop	1,000,000	2,000,000	50%
HP - HX B•22-•••	Safety hinges	1,000,000	5,000,000	20%
SR	Magnetic safety sensors (with compatible Pizzato Elettrica safety modules)	20,000,000	20,000,000	50%
SR	Magnetic safety sensors (with max load: DC12 24V 250mA)	400,000	400,000	100%
PX, PA	Foot switches	1,000,000	20,000,000	50%
MK	Micro position switches	1,000,000	20,000,000	50%
NA, NB, NF	Modular pre-wired position switches	1,000,000	40,000,000	50%
E2 C•••••••	Contact blocks	1,000,000	40,000,000	50%

Series	Article description	B_{10D}	B_{10}/B_{10D}
E2 •PU1••••••, E2 •PL1••••••	Single buttons, maintained	2,000,000	50%
E2 •PU2••••••, E2 •PL2••••••	Single buttons, spring-return	30,000,000	50%
E2 •PD••••••, E2 •PT••••••	Double and triple buttons	2,000,000	50%
E2 •PQ••••••	Quadruple buttons	2,000,000	50%
E2 •PE••••••	Emergency stop buttons	600,000	50%
VN NG-AC2605•	Emergency stop buttons integrated on NG series safety switches	100.000	50%
E2 •SE••••••, E2 •SL••••••	Selector switches with and without illumination	2,000,000	50%
E2 •SC••••••	Key selector switches	600,000	50%
E2 •MA••••••	Joysticks	2,000,000	50%

ATEX series	Article description	B_{10D} (NO)	B_{10D} (NC)	B_{10}/B_{10D}
F• ••••-EX•	Position switches	500,000	20,000,000	50%
F• ••93-EX• F• ••92-EX•	Safety switches with separate actuator	500,000	1,000,000	50%
F• ••99-EX• F• ••R2-EX•	Safety switches with separate actuator with lock	500,000	500,000	50%
F• ••96-EX• F• ••95-EX•	Safety switch with hinge pin	500,000	2,500,000	20%
F• ••C•-EX•	Switches with slotted hole lever for hinged guards	500,000	1,000,000	50%
F• ••••-EX•	Rope switches for emergency stop	500,000	1,000,000	50%

Electronic devices

Code/series	Article description	$MTTF_D$	DC	PFH_D	SIL CL	PL	Cat
HX BEE1-•••	Safety hinge with electronic unit	2413	H	1.24E-09	3	e	4
ST	Safety sensors with RFID technology	4077	H	1.20E-11	3	e	4
NG	RFID safety switches with lock (mode 1 / mode 2)	2725	H	1,17E-09	3	e	4
NG	RFID safety switches with lock (mode 3)	2511	H	1,84E-09	2	d	2
NG	RFID safety switches with lock (two-channel monitoring of the guard locking function)	4011	H	1,51E-10	3	e	4
NG	RFID safety switches with lock (single-channel monitoring of the guard locking function)	4011	H	1,51E-10	2	d	2
NS	RFID safety switches with lock (mode 1 / mode 2)	1671	H	1.24E-09	3	e	4
NS	RFID safety switches with lock (mode 3)	1677	H	1.82E-09	2	d	2
NS	RFID safety switches with lock (two-channel monitoring of the guard locking function)	2254	H	2.04E-10	3	e	4
NS	RFID safety switches with lock (single-channel monitoring of the guard locking function)	2254	H	2.04E-10	2	d	2
CS AM-01	Safety module for standstill monitoring	218	M	8.70E-09	2	d	3
CS AR-01, CS AR-02	Safety modules for monitoring guards and emergency stops	227	H	1.18E-10	3	e	4

B_{10D}: Number of operations after which 10% of the components have failed dangerously
B_{10}: Number of operations after which 10% of the components have failed
B_{10}/B_{10D}: ratio of total failures to dangerous failures.
$MTTF_D$: Mean Time To Dangerous Failure

DC: Diagnostic Coverage
PFH_D: Probability of Dangerous Failure per hour
SIL CL: Safety Integrity Level Claim Limit. Maximum achievable SIL according to EN 62061
PL: Performance Level. PL acc. to EN ISO 13849-1

Electronic devices

Code/series	Article description	$MTTF_D$	DC	PFH_D	SIL CL	PL	Cat
CS AR-04	Safety module for monitoring guards and emergency stops	152	H	1.84E-10	3	e	4
CS AR-05, CS AR-06	Safety modules for monitoring guards, emergency stops and light barriers	152	H	1.84E-10	3	e	4
CS AR-07	Safety module for monitoring guards and emergency stops	111	H	7.56E-10	3	e	4
CS AR-08	Safety module for monitoring guards, emergency stops and light barriers	1547	H	9.73E-11	3	e	4
CS AR-20, CS AR-21	Safety modules for monitoring guards and emergency stops	225	H	4.18E-10	3	e	3
CS AR-22, CS AR-23	Safety modules for monitoring guards and emergency stops	151	H	5.28E-10	3	e	3
CS AR-24, CS AR-25	Safety modules for monitoring guards and emergency stops	113	H	6.62E-10	3	e	3
CS AR-40, CS AR-41	Safety modules for monitoring guards and emergency stops	225	H	4.18E-10	2	d	2
CS AR-46	Safety module for monitoring guards and emergency stops	435	-	3.32E-08	1	c	1
CS AR-51	Safety module for monitoring safety mats and safety bumpers	212	H	3.65E-09	3	e	4
CS AR-90	Safety module for monitoring floor leveling in lifts	382	H	5.03E-10	3	e	4
CS AR-91	Safety module for monitoring floor leveling in lifts	227	H	1.18E-10	3	e	4
CS AR-93	Safety module for monitoring floor leveling in lifts	227	H	1.34E-10	3	e	4
CS AR-94	Safety module for monitoring floor leveling in lifts	227	H	1.13E-10	3	e	4
CS AR-94•U12	Safety module for monitoring floor leveling in lifts	227	H	1.13E-10	3	e	4
CS AR-95	Safety module for monitoring floor leveling in lifts	213	H	5.42E-09	3	e	4
CS AT-0•, CS AT-1•	Safety modules with timer for monitoring guards and emergency stops	88	H	1.23E-08	3	e	4
CS AT-3•	Safety module with timer for monitoring guards and emergency stops	135	H	1.95E-09	3	e	4
CS DM-01	Safety module for monitoring two-hand controls	142	H	2.99E-08	3	e	4
CS DM-02	Safety module for monitoring two-hand controls	206	H	2.98E-08	3	e	4
CS DM-20	Safety module for monitoring two-hand controls	42	-	1.32E-06	1	c	1
CS FS-1•	Safety timer module	404	H	5.06E-10	3	e	4
CS FS-2•, CS FS-3•	Safety timer modules	205	H	1.10E-08	2	d	3
CS FS-5•	Safety timer module	379	M	1.31E-09	2	d	3
CS ME-01	Contact expansion module	91	H	5.26E-10	①	①	①
CS ME-02	Contact expansion module	114	H	4.17E-10	①	①	①
CS ME-03	Contact expansion module	152	H	3.09E-10	①	①	①
CS ME-20	Contact expansion module	114	H	6.14E-10	①	①	①
CS ME-3•	Contact expansion module	110	H	4.07E-09	①	①	①
CS M•201	Multifunction safety modules	135	H	1.44E-09	3	e	4
CS M•202	Multifunction safety modules	614	H	1.32E-09	3	e	4
CS M•203	Multifunction safety modules	103	H	1.61E-09	3	e	4
CS M•204	Multifunction safety modules	134	H	1.52E-09	3	e	4
CS M•205	Multifunction safety modules	373	H	2.19E-09	3	e	4
CS M•206	Multifunction safety modules	3314	H	1.09E-09	3	e	4
CS M•207	Multifunction safety modules	431	H	7.08E-09	3	e	4
CS M•208	Multifunction safety modules	633	H	7.02E-09	3	e	4
CS M•301	Multifunction safety modules	128	H	1.88E-09	3	e	4
CS M•302	Multifunction safety modules	535	H	1.57E-09	3	e	4
CS M•303	Multifunction safety modules	485	H	1.76E-09	3	e	4
CS M•304	Multifunction safety modules	98	H	2.05E-09	3	e	4
CS M•305	Multifunction safety modules	535	H	1.57E-09	3	e	4
CS M•306	Multifunction safety modules	100	H	1.86E-09	3	e	4
CS M•307	Multifunction safety modules	289	H	8.38E-09	3	e	4
CS M•308	Multifunction safety modules	548	H	7.27E-09	3	e	4
CS M•309	Multifunction safety modules	496	H	7.46E-09	3	e	4
CS M•401	Multifunction safety modules	434	H	1.73E-09	3	e	4
CS M•402	Multifunction safety modules	478	H	7.24E-09	3	e	4
CS M•403	Multifunction safety modules	438	H	7.42E-09	3	e	4

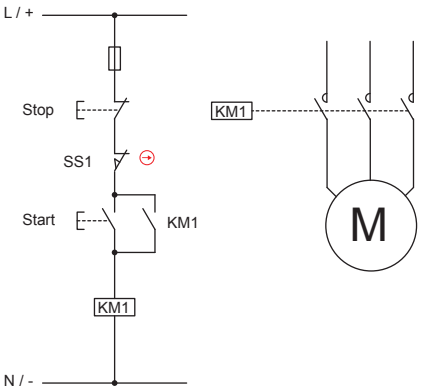
B_{10D}: Number of operations after which 10% of the components have failed dangerously
B_{10}: Number of operations after which 10% of the components have failed
B_{10}/B_{10D}: ratio of total failures to dangerous failures.
$MTTF_D$: Mean Time To Dangerous Failure

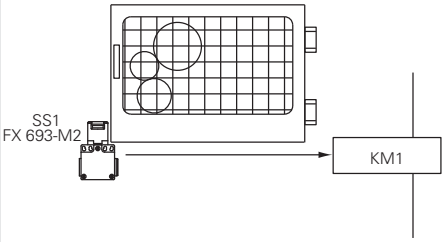
DC: Diagnostic Coverage
PFH_D: Probability of Dangerous Failure per hour
SIL CL: Safety Integrity Level Claim Limit. Maximum achievable SIL according to EN 62061
PL: Performance Level. PL acc. to EN ISO 13849-1

① = Depending on the base module

EXAMPLE 1
Application: Guard monitoring

Reference standard EN ISO 13849-1	
Safety category	**1**
Performance Level	**PL c**





Description of the safety function
The control circuit illustrated above has a guard monitoring function. If the guard is open the engine must not be able to start. The hazard analysis showed that the system has no inertia or rather that the engine, once the power has been switched off, stops at a much faster rate than the opening of the guard. The risk analysis has shown that the required PL_r target is PL c. This is necessary to verify if the intended control circuit with single channel structure is provided with a PL higher or equal to PL_r.
The guard position is detected by the switch with separate actuator SS1, which operates directly on the contactor KM1. The contactor KM1 monitoring the moving parts is usually activated by the Start and Stop buttons. Though, the analysis of the working cycle has shown that the guard is opening at every switching operation too. Therefore, the number of switch operations by the contactor and by the safety switch can be considered equal.
A circuit structure is defined as single-channel without supervision (category B or 1) if there are only an Input component (switch) and an Output (contactor) component.
In case a failure on one of the two devices the safety function is not guaranteed anymore.
No measures for fault detection have been applied.

Device data:
- SS1 (FX 693-M2) is a switch with positive opening (in accordance with EN 60947-5-1, Annex K). The switch is a well-tried component according to EN ISO 13849-2 table D.4. The B_{10D} value of the device supplied by the manufacturer is equal to 2,000,000 switching operations.
- KM1 is a contactor operated at nominal load and is a well-tried component in compliance with EN ISO 13849-2, table D.4. The B_{10D} value of this component is equal to 1,300,000 switching operations. This value results from the tables of the applicable standard (see EN ISO 13849-1, table C.1).

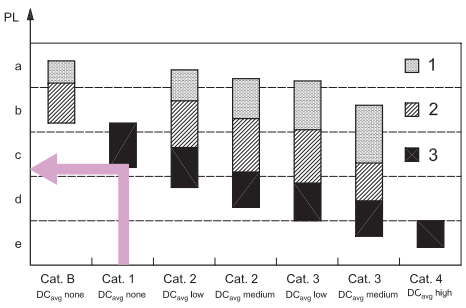
Assumption of the frequency of use
- It is assumed that the equipment is used for a maximum of 365 days per year, for three shifts of 8 hours and 600 s cycle time. For the switch, the number of switching operations per year is equal to maximum N_{op}=(365x24x3,600)/600=52,560.
- It is assumed that the start button is operated every 300 seconds. Therefore, the maximum number of switching operations per year is equal to n_{op}/year=105,120
- The contactor KM1 is actuated both for the normal start-stop of the machine as well as for the restart after a guard opening. n_{op}/year=52,560+105,120 = 157,680

$MTTF_D$ calculation
The $MTTF_D$ of the SS1 switch is equal to: $MTTF_d = B_{10D}/(0,1 \times n_{op})$ = 2,000,000/(0,1 x 52560) = 381 years
The$MTTF_D$ of the KM1 contactor is equal to: $MTTF_D = B_{10D}/(0.1 \times n_{op})$ = 1,300,000/(0.1 x 157680) = 82 years
Therefore, the $MTTF_D$ of the single-channel circuit is equal to: 1/(1/381+1/82) = 67 years

Diagnostic Coverage DCavg
No measures for fault detection have been applied and there is therefore no diagnostic coverage, a permissible condition for the circuit in question that is in category 1.

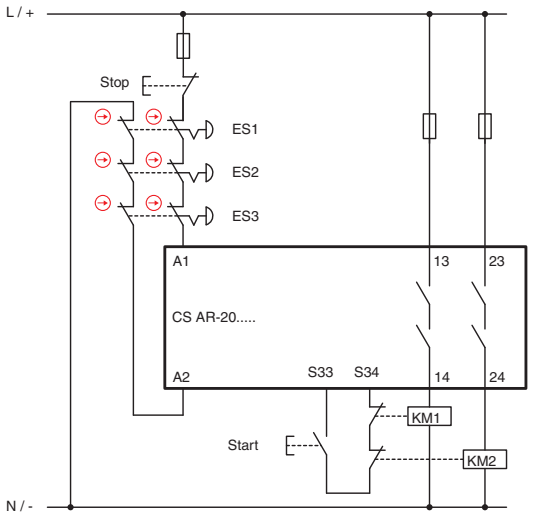
CCF Common Cause Failures
The CCF calculation is not required for category 1 circuits.

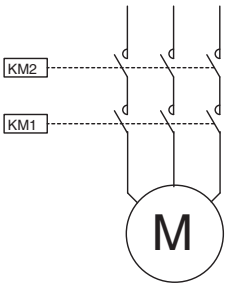
PL determination
Using the graph or the figure no. 5 of the standard, it can be verified that for a Category 1 circuit with $MTTF_D$ = 95 years the resulting PL of the control circuit is PL c. The PL_r target is therefore achieved.

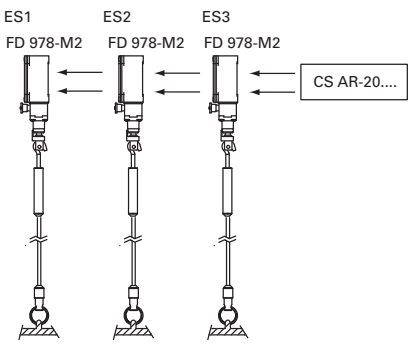


EXAMPLE 2
Application: Emergency stop control

Reference standard EN ISO 13849-1	
Safety category	**3**
Performance Level	**PL e**







Description of the safety function
The operation of one of the emergency devices causes the intervention of the safety module and the two contactors KM1 and KM2. The signal of the devices ES1, ES2, ES3 is redundantly read by the CS safety module. The contactors KM1 and KM2 (with forcibly guided contacts) are monitored by the CS via the feedback circuit too.

Device data:
- The devices ES1, ES2, ES3 (FD 978-M2) are rope switches for emergency stop with positive opening. The B10D value is 2,000,000
- KM1 and KM2 are contactors operated at nominal load. The B10D value is 1,300,000 (see EN ISO 13849-1 - Table C.1)
- CS is a safety module (CS AR-20) with $MTTF_D$ = 225 years and DC = High
- The circuit structure is two-channel in category 3

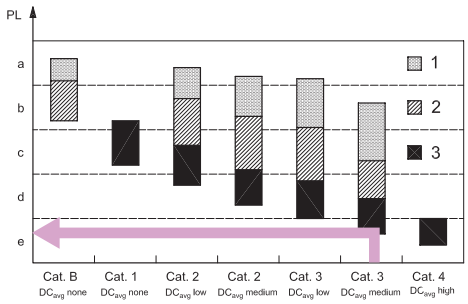
Assumption of the frequency of use
- Twice a month, nop/year = 24
- Start button actuation: 4 times a day
- Assuming 365 working days, the contactors will take action 4 x 365 + 24 = 1484 times / year
- The switches will be operated with the same frequency.
- It is not expected that multiple buttons will be pressed simultaneously.

$MTTF_D$ calculation
- $MTTF_{D\ ES1,ES2,ES3}$ = 833,333 years
- $MTTF_{D\ KM1,KM2}$ = 8760 years
- $MTTF_{D\ CS}$ = 225 years
- $MTTF_{D\ ch1}$ = 219 years. The value must be limited to 100 years. The channels are symmetric, therefore $MTTF_D$ = 100 years (High)
-

Diagnostic Coverage DC_{avg}
- The contacts of KM1 and KM2 are monitored by the CS module via the feedback circuit. DC=99% (High)
- The safety module CS AR-20 is provided with a "High" diagnostic coverage.
- Not all failures in the series of emergency devices can be detected. The diagnostic coverage is 90% (Medium)

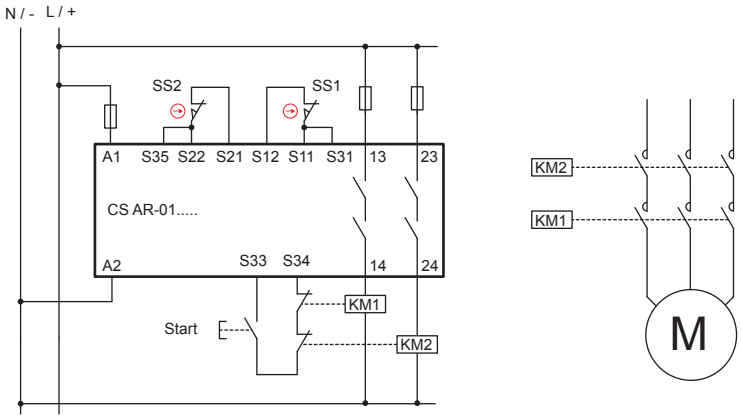
CCF Common Cause Failures
We assume a score > 65 (acc. to EN ISO 13849-1 - Annex F).

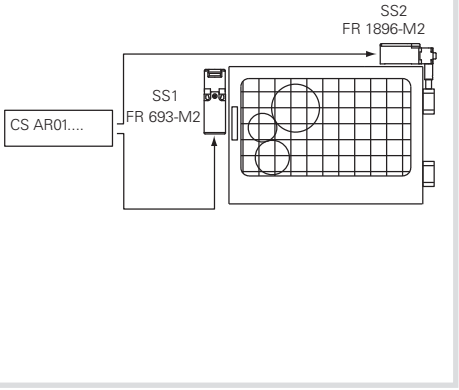
PL determination
A circuit in category 3 with $MTTF_D$=High and DC_{avg}= High can reach a PL e.



EXAMPLE 3
Application: Guard monitoring

Reference standard EN ISO 13849-1	
Safety category	**4**
Performance Level	**PL e**





Description of the safety function
The guard opening causes the intervention of the switches SS1 and SS2 and, by consequence, of the safety module and the KM1 and KM2 contactors too
The signal of the devices SS1 and SS2 is redundantly monitored by the CS safety module.
The switches have different operating principles.
The contactors KM1 and KM2 (with forcibly guided contacts) are monitored by the CS via the feedback circuit too.

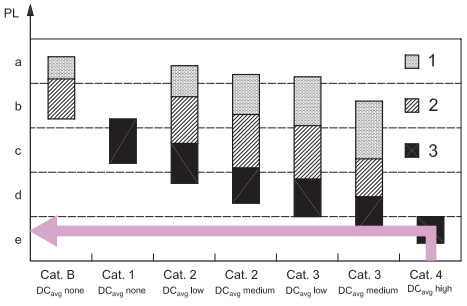
Device data:
- The switch SS1 (FR 693-M2) is a switch with positive opening. The B_{10D} value is 2,000,000
- The switch SS2 (FR 1896-M2) is a hinge switch with positive opening. B_{10D}= 5,000,000
- KM1 and KM2 are contactors operated at nominal load. B_{10D} = 1,300,000 (see EN ISO 13849-1 - Table C.1)
- The CS modules are safety modules (CS AR-01) with $MTTF_D$ = 227 years and DC = High

Assumption of the frequency of use
365 days/year, 16 h/day, 1 action every 4 minutes (240 s). n_{op}/year = 87,600.

$MTTF_D$ calculation
- $MTTF_{D\ SS1}$ = 228 years
- $MTTF_{D\ SS2}$ = 571 years
- $MTTF_{D\ KM1,KM2}$ = 148 years
- $MTTF_{D\ CS}$ = 227 years
- $MTTF_{D\ CH1}$ = 64 years (SS1,CS,KM1)
- $MTTF_{D\ CH2}$ = 77 years (SS2,CS,KM2)
- $MTTF_D$: by calculating the average of the two channels $MTTF_D$ = 70.7 years (High) is achieved
-

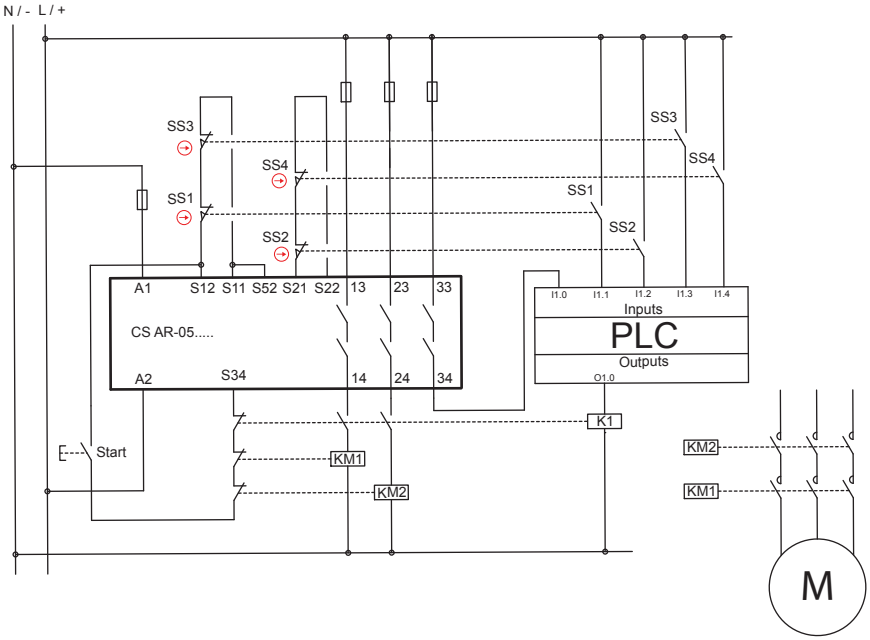
Diagnostic Coverage DC_{avg}
- SS1 and SS2 have DC = 99% since the SS1 and SS2 contacts are monitored by CS and have different operation principles.
- The contacts of KM1 and KM2 are monitored by the CS module via the feedback circuit. DC=99% (High)
- CS AR-01 is provided with an internal redundant and self-monitoring circuit. DC = High
- DC_{avg}= High

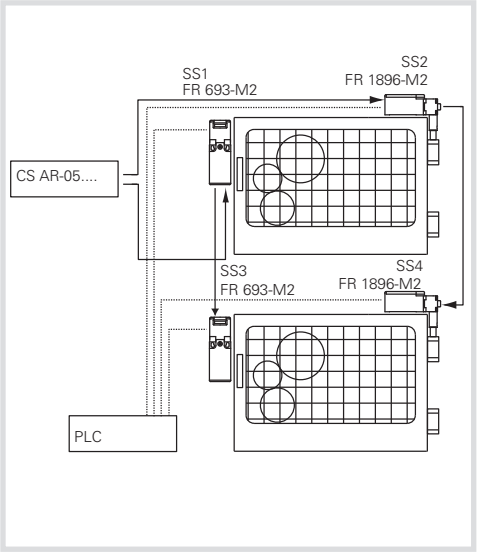
PL determination
A circuit in category 4 with $MTTF_D$ = 72.1 years and DC_{avg} = High corresponds to PL e.



EXAMPLE 4
Application: Guard monitoring

Reference standard EN ISO 13849-1	
Safety category	**4**
Performance Level	**PL e**





Description of the safety function
The opening of a guard triggers switches SS1 and SS2 on the first guard and triggers SS3, SS4 on the second; the switches trigger the safety module and both contactors KM1 and KM2.
The signal of the devices SS1, SS2 and SS3, SS4 is redundantly monitored by the CS safety module. Furthermore, an auxiliary contact of the switch is monitored by the PLC.
The switches have different operating principles.
The contactors KM1 and KM2 (with forcibly guided contacts) are monitored by the CS via the feedback circuit too.

Device data:
- The switches SS1, SS3 (FR 693-M2) are switches with positive opening. The B_{10D} value is 2,000,000
- The switches SS2, SS4 (FR 1896-M2) are hinge switches with positive opening. B_{10D}= 5,000,000
- KM1 and KM2 are contactors operated at nominal load. The B_{10D} value is 1,300,000 (see EN ISO 13849-1 - Table C.1)
- CS is a safety module (CS AR-05) with $MTTF_D$ = 152 years and DC = High

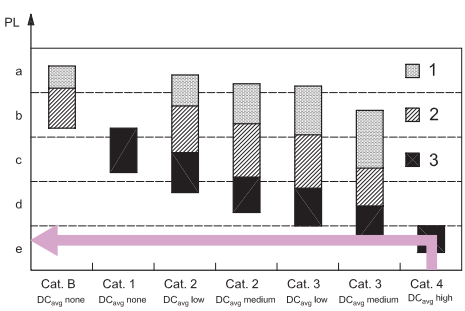
Assumption of the frequency of use
- 4 times per hour for 24 h/day for 365 days/year equal to n_{op}/year = 35,040
- The contactors will operate for twice the number of operations = 70,080

$MTTF_{d\ calculation}$
- $MTTF_{D\ SS1,SS3}$ = 571 years; $MTTF_{D\ SS2,SS4}$ = 1,427 years
- $MTTF_{D\ KM1,KM2}$ = 185 years
- $MTTF_{D\ CS}$ = 152 years
- $MTTF_{D\ Ch1}$ = 73 years (SS1, CS, KM1) / (SS3, CS, KM1)
- $MTTF_{D\ Ch2}$ = 79 years (SS2, CS, KM2) / (SS4, CS, KM2)
- $MTTF_D$: by calculating the average of the two channels $MTTF_D$ = 76 years (High) is achieved

Diagnostic Coverage DC_{avg}
- The contacts of KM1, KM2 are monitored by the CS module via the feedback circuit. DC=99%
- All auxiliary contacts of the switches are monitored by the PLC. DC=99%
- The CS AR-05 module has a DC= High
- The diagnostic coverage for both channels is 99% (High)

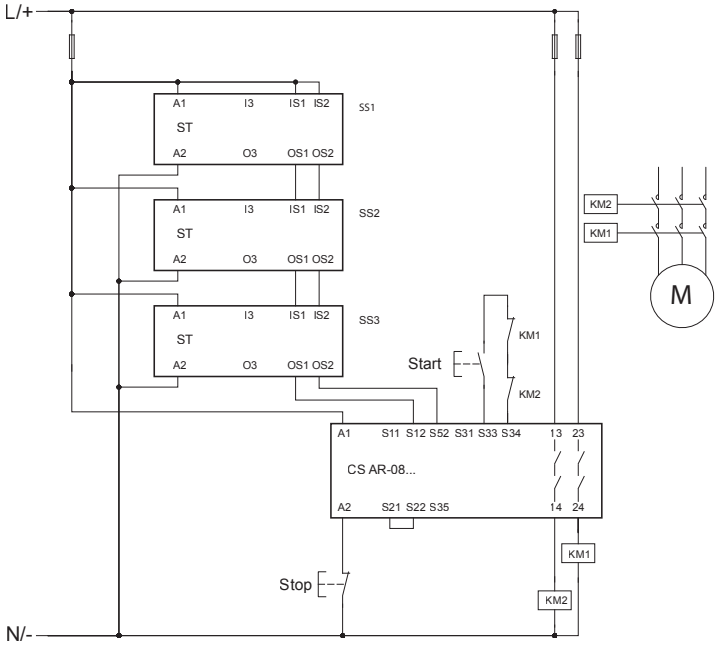
CCF Common Cause Failures
- We assume a score > 65 (acc. to EN ISO 13849-1 - Annex F).

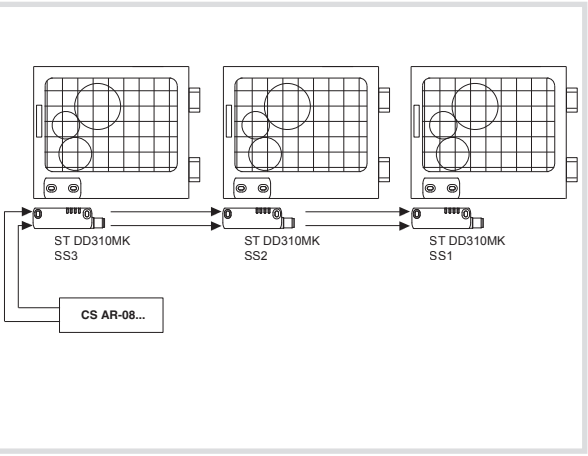
PL determination
- A circuit in category 4 with $MTTF_D$ = 88.6 years (High) and DC_{avg} = High corresponds to PL e.



EXAMPLE 5
Application: Guard monitoring

Reference standard EN ISO 13849-1	
Safety category	**4**
Performance Level	**PL e**

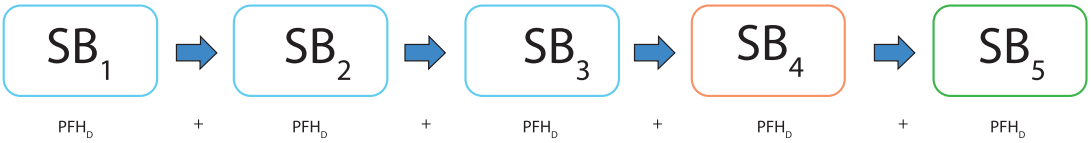




Description of the safety function
The opening of guards triggers the sensors SS1 on the first guard, SS2 on the second and SS3 on the third. The sensors trigger the safety module CS AR-08 and the contactors KM1 and KM2 too. The contactors KM1 and KM2 (with forcibly guided contacts) are monitored by the CS AR-08 via the feedback circuit.

Device data
SS1, SS2, SS3 are ST series coded sensors with RFID technology. PFH_D = 1.20E-11, PL = "e"
CS AR-08 is a safety module. PFH_D = 9.73E-11, PL = "e"
KM1 and KM2 are contactors operated at nominal load. B_{10D} = 1,300,000 (see EN ISO 13849-1 - Table C.1)

Assumption of the frequency of use
Each door is opened every 2 minutes, 16 hours a day, for 365 days a year, equal to nop = 175,200
Definition of the SRP/CS and subsystems
The SRP/CS consists of 5 subsystems (SB):
SB1,2,3 represent the three ST series RFID sensors
SB4 represents the safety module CS AR-08...
SB5 represents the two contactors KM1 and KM2 in redundant architecture (cat. 4)



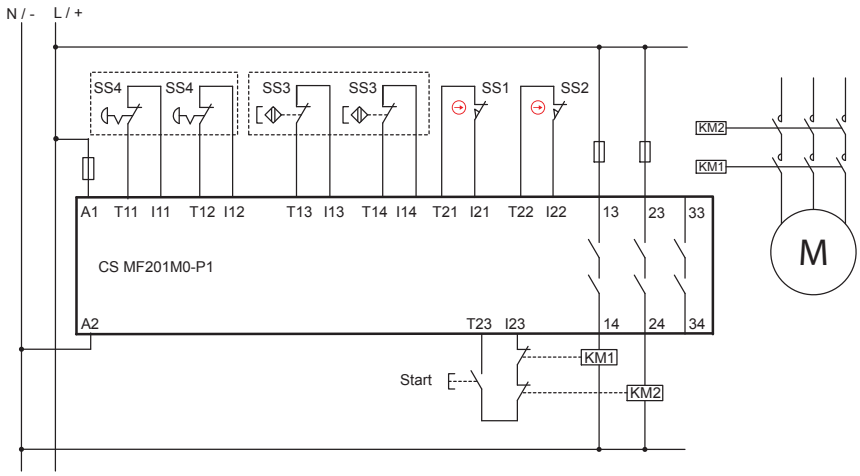
PFH_D calculation for SB5
$MTTF_D$ KM1,KM2 = 74.2 years.
DC = 99%, the contacts of KM1 and KM2 are monitored by the CS safety module via the feedback circuit.
For the CCF parameter we assume a score higher than 65 (acc. to EN ISO 13849-1 - Annex F).
A category 4 circuit with $MTTF_D$ = 74.2 years (high) and high diagnostic coverage (DC = 99%) corresponds to a failure probability of PFH_D = 3.4E-08 and a PL "e".

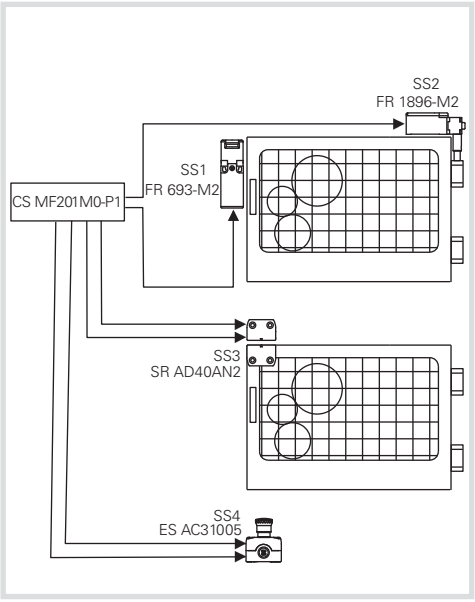
Calculation of the total PFH_D of the SRP/CS
$PFH_{DTOT} = PFH_{DSB1} + PFH_{DSB2} + PFH_{DSB3} + PFH_{DSB4} + PFH_{DSB5}$ = 3.5E-08
It corresponds to PL "e".

Calculation example performed with SISTEMA software, downloadable free of charge at www.pizzato.com

EXAMPLE 6
Application: Guard monitoring

Reference standard EN ISO 13849-1	
Safety category	4
Performance Level	PL e





Description of the safety function
The opening of a guard triggers switches SS1 and SS2 on the first guard and triggers sensor SS3 on the second; the switches trigger the safety module and both contactors KM1 and KM2.
The signals from the SS1, SS2 and SS3 devices are redundantly monitored by the CS MF safety module.
There is also an emergency stop button which has a two-channel connection with the safety module too.
The contactors KM1 and KM2 (with forcibly guided contacts) are monitored by the CS MF via the feedback circuit too.

Device data:
- The switch SS1 (FR 693-M2) is a switch with positive opening. B_{10D} = 2,000,000
- The switch SS3 (FR 1896-M2) is a hinge switch with positive opening. B_{10D}= 5,000,000
- SS3 (SR AD40AN2) is a magnetic safety sensor. B_{10D} = 20,000,000
- SS4 (ES AC31005) is a housing with emergency stop button (E2 1PERZ4531) provided with 2 NC contacts. B_{10D}= 600,000
- KM1 and KM2 are contactors operated at nominal load. B_{10D} = 1,300,000 (see EN ISO 13849-1 - Table C.1)
- CS MF201M0-P1 is a safety module with $MTTF_D$ = 842 years and DC = 99%

Assumption of the frequency of use
- Each door is opened 2 times per hour for 16 h/day for 365 days/year equal to n_{op}/year = 11,680
- It is assumed that the emergency button is actuated at a maximum of once a day, n_{op}/year = 365
- The contactors will operate for twice the number of operations = 23,725

$MTTF_D$ calculation

Guard SS1/SS2
- $MTTF_{D\ SS1,SS3}$ = 1,712 years
- $MTTF_{D\ SS2,SS4}$ = 4,281 years
- $MTTF_{D\ KM1,KM2}$ = 548 years
- $MTTF_{D\ CS}$ = 842 years
- $MTTF_{D\ CH1}$ = 278 years (SS1, CS, KM1)
- $MTTF_{D\ CH2}$ = 308 years (SS2, CS, KM2)
- $MTTF_D$ = by calculating the average of the two channels $MTTF_D$ = 293 years is achieved

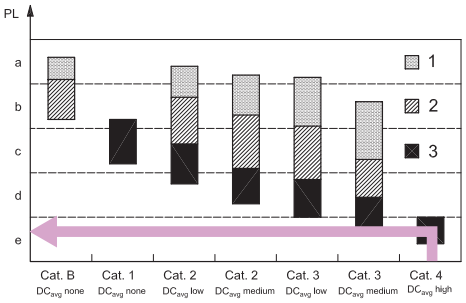
Guard SS3
- $MTTF_{D\ SS3}$ = 17,123 years
- $MTTF_{D\ KM1,KM2}$ = 548 years
- $MTTF_{D\ CS}$ = 842 years
- $MTTF_D$ = 325 years

Emergency stop button SS4
- $MTTF_{D\ SS4}$ = 16,438 years
- $MTTF_{D\ KM1,KM2}$ = 548 years
- $MTTF_{D\ CS}$ = 842 years
- $MTTF_D$ = 325 years

Diagnostic Coverage DC_{avg}
- The contacts of KM1, KM2 are monitored by the CS MF module via the feedback circuit. DC=99%
- For the devices SS1, SS2 and SS3 it is possible to detect all faults. DC=99%
- The CS MF201M0-P1 module has a DC=99%
- We assume a diagnostic coverage of 99% (High)

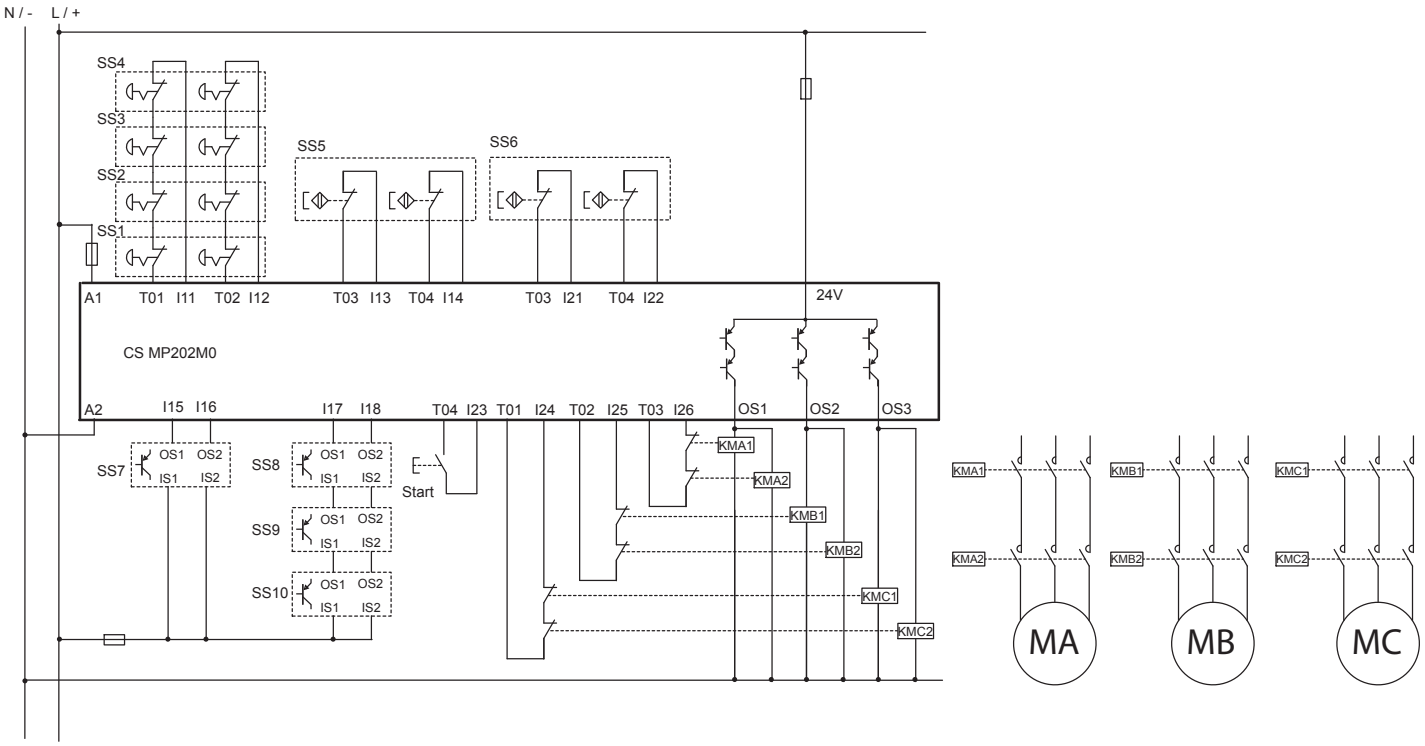
CCF Common Cause Failures
- We assume a score > 65 (acc. to EN ISO 13849-1 - Annex F).

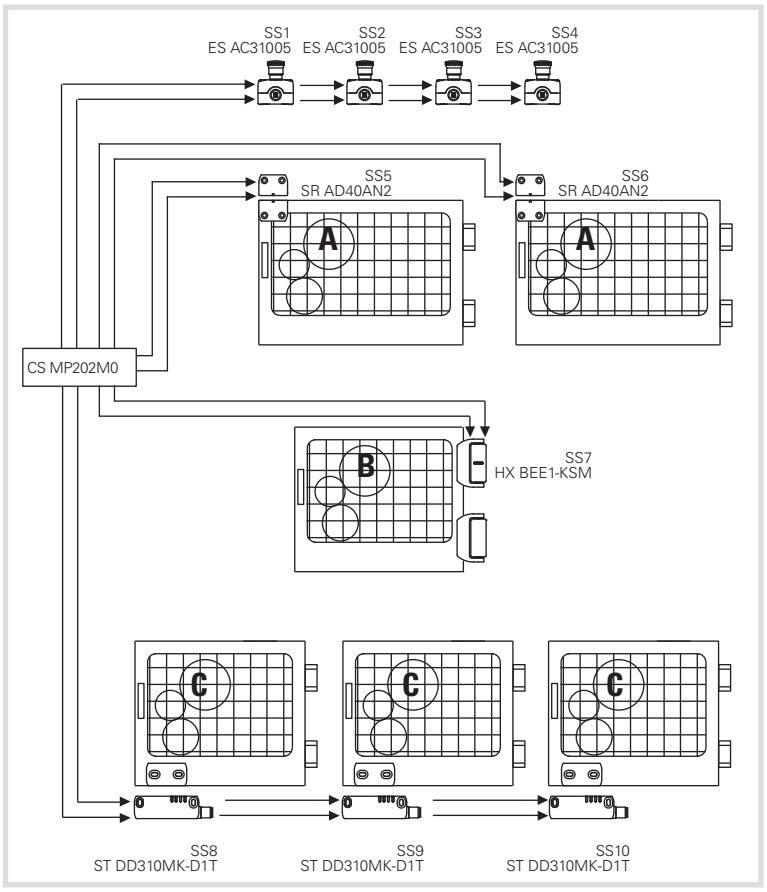
PL determination
- A circuit in category 4 with $MTTF_D \geq 30$ years (High) and DC_{avg} = High corresponds to PL e.
- The safety functions associated to the guards SS1/SS2, SS3 and the emergency stop button present the level PL e.

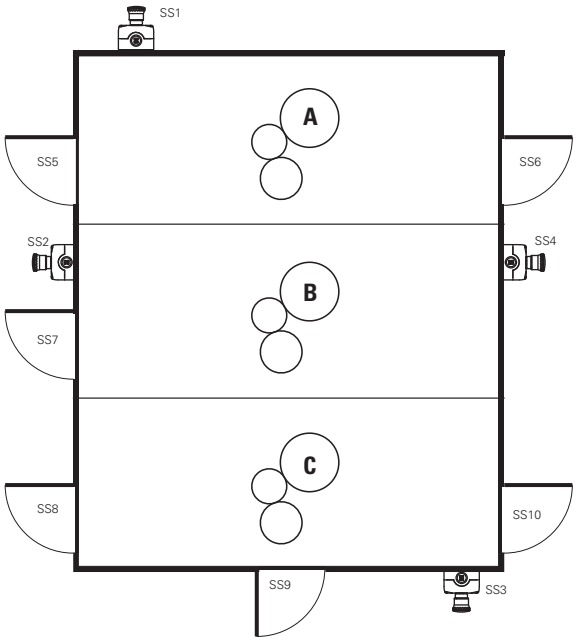


EXAMPLE 7
Application: Guard monitoring

Reference standard EN ISO 13849-1	
Safety category	**4**
Performance Level	**PL e**







Description of the safety function

Every machine is divided into 3 different zones. The access to each zone is monitored by the guards and 4 emergency stop buttons are present too.
The operation of an emergency stop button will trigger the CS MP safety module as well as the forcibly guided contactors KMA1/2, KMB1/2 and KMC1/2, and will therefore stop all motors.
The opening of a guard in zone A triggers the devices SS5 or SS6 and, as a consequence, the CS MP safety module as well as the contactors KMA1 and KMA2, and therefore also the stop of the MA motor. The devices SS5 and SS6 are connected to the CS MP safety module separately, with a two-channel connection.
The opening of the guard in zone B triggers the device SS7 and, as a consequence, the CS MP safety module as well as the contactors KMB1 and KMB2, and therefore also the stop of the MB motor. The SS7 hinge is provided with two OSSD outputs and is redundantly controlled by the CS MP safety module.
The opening of a guard in zone C triggers the devices SS8, SS9 or SS10 and, as a consequence, the safety module as well as the contactors KMC1 and KMC2, and therefore also the stop of the MC motor. The sensors SS8, SS9 and SS10 are interconnected via the OSSD outputs and are redundantly monitored by the CS MP safety module.

Device data

- SS1, SS2, SS3 and SS4 (ES AC31005) are emergency stop buttons (E2 1PERZ4531) provided with 2 NC contacts. B_{10D} = 600,000
- SS5 and SS6 (SR AD40AN2) are magnetic safety sensors. B_{10D} = 20,000,000
- SS7 (HX BEE1-KSM) is a safety hinge with OSSD outputs. $MTTF_D$ = 4,077 years / DC = 99%
- SS8, SS9 and SS10 (ST DD310MK-D1T) are safety sensors with RFID technology and OSSD outputs. $MTTF_D$ = 4,077 years / DC = 99%
- KMA, KMB and KMC are contactors operated at nominal load. B_{10D} = 1,300,000 (see EN ISO 13849-1 - Table C.1)
- CS MP202M0 is a safety module with $MTTF_D$ = 2035 years / DC = 99%

Assumption of the frequency of use

- Each door of zone A is opened 2 times per hour for 16 h/day for 365 days/year equal to n_{op}/year = 11,680. The contactors will operate for twice the number of operations = 23,360
- The door of zone B is opened 4 times per hour for 16 h/day for 365 days/year equal to n_{op}/year = 23,360. The contactors will operate for a given number of operations = 23,360
- Each door of zone C is opened 1 times per hour for 16 h/day for 365 days/year equal to n_{op}/year = 5,840. The contactors will operate for a given number of operations = 17,520
- It is assumed that the emergency button is actuated at a maximum of once a week, n_{op}/year = 52
- Fault Exclusion: since it is assumed that the pairs of contactors, connected in parallel to the respective safety outputs, are wired permanently within the switching cabinet, the possibility of short-circuit between +24V and the contactors is excluded (see Table D.4, item D.5.2 of EN ISO 13849-2).

$MTTF_D$ calculation

Emergency stop buttons

- $MTTF_D$ SS1/SS2/SS3/SS4 = 115,384 years
- $MTTF_D$ CS = 2035 years
- $MTTF_D$ KMC1,KMC2 = 742 years
- $MTTF_D$ e-stop = 541 years

Guards, zone A

- $MTTF_D$ SS5/SS6 = 17,123 years
- $MTTF_D$ CS = 2035 years
- $MTTF_D$ KMA1,KMA2 = 556 years
- $MTTF_D$ A = 425 years (SS5/SS6,CS,KMA)

Guards, zone B

- $MTTF_D$ SS7 = 4,077 years
- $MTTF_D$ CS = 2035 years
- $MTTF_D$ KMB1,KMB2 = 556 years
- $MTTF_D$ B = 394 years (SS7,CS,KMB)

Guards, zone C

- $MTTF_D$ SS8/SS9/SS10 = 4,077 years
- $MTTF_D$ CS = 2035 years
- $MTTF_D$ KMC1,KMC2 = 742 years
- $MTTF_D$ C = 479 years (SS8/SS9/SS10,CS,KMC)

Diagnostic Coverage DC_{avg}

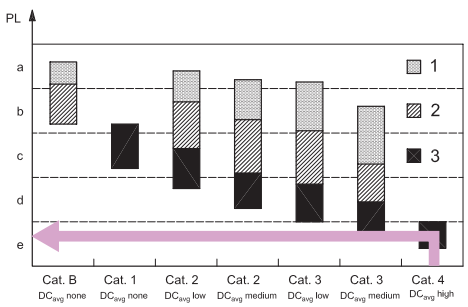
- The contacts of KMA, KMB and KMC are monitored by the CS MP module via the feedback circuit. DC=99%
- All faults in the various devices can be detected. DC=99%
- The CS MP202M0 module has a DC=99%
- The result is a diagnostic coverage of 99% for each function

CCF Common Cause Failures

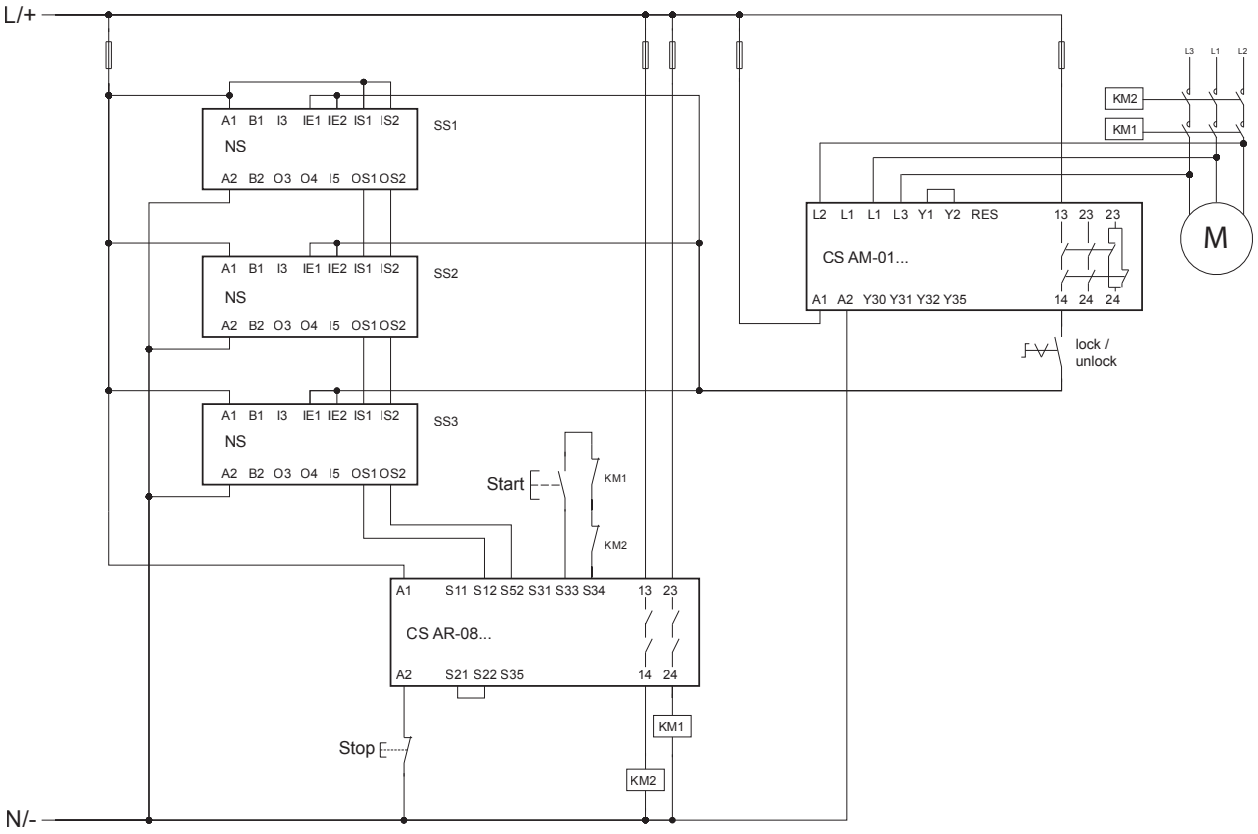
- We assume a score > 65 for all safety functions (acc. to EN ISO 13849-1 - Annex F).

PL determination

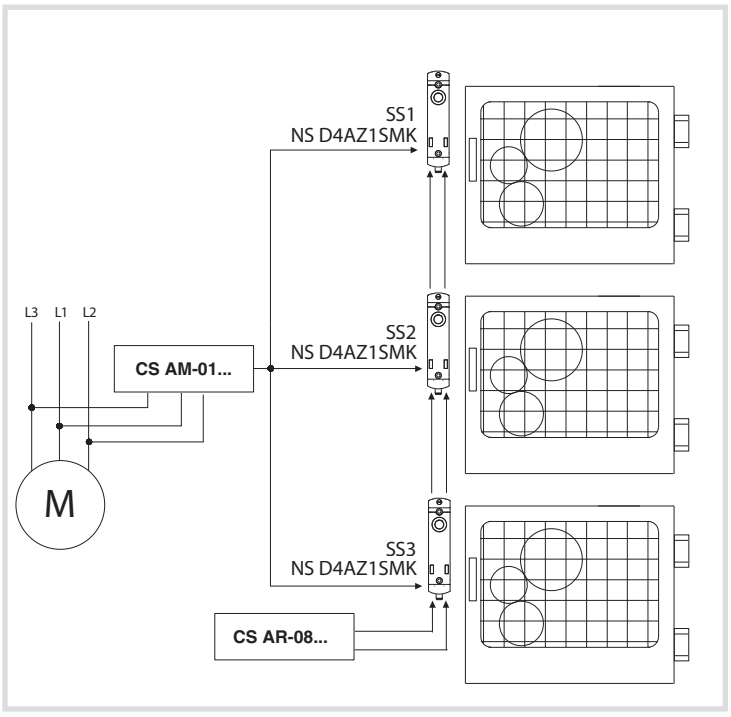
- A circuit in category 4 with $MTTF_D \geq 30$ years (High) and DC_{avg} = High corresponds to PL e.
- All safety functions associated to the guards and the emergency stop buttons have PL e.



EXAMPLE 8
Application: Guard monitoring



Reference standard EN ISO 13849-1	
Performance Level - Safety function 1	**PL e**
Performance Level - Safety function 2	**PL d**

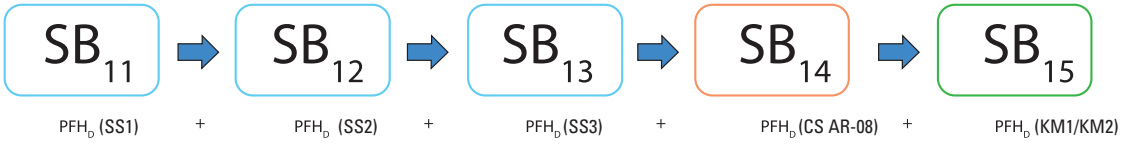


Description of the safety function
Interlocking devices SS1, SS2 and SS3 perform two safety functions: monitoring the locked state and locking the guard.
Once the guards have been released, the three sensors trigger the safety module and the contactors KM1 and KM2 too. The contactors KM1 and KM2 (with forcibly guided contacts) are monitored by the CS AR-08 via the feedback circuit.
The interlock command on the three devices SS1, SS2 and SS3 is maintained until the motor standstill monitoring module CS AM-01 detects the actual stopping of movement.

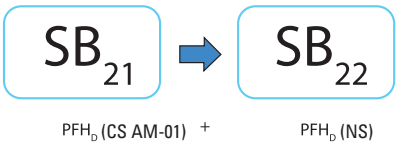
Device data
SS1, SS2, SS3 are NS series coded interlock devices with RFID technology, with guard locking device. Locked protection detection function PFH_D = 1.22E-09 PL = "e", operating of locking control PFH_D = 2.29E-10 PL = "e".
CS AR-08 is a safety module, PFH_D = 9.73 E-11, PL = "e".
CS AM-01 is a safety module for motor standstill monitoring, PFH_D = 8,70E-09, PL "d".
KM1 and KM2 are contactors operated at nominal load. $B10_D$ = 1,300,000 (see EN ISO 13849-1 - Table C.1)

Assumption of the frequency of use
Each door is opened every 10 minutes, 16 hours a day, for 365 days a year, equal to n_{op}/year = 35,040

Definition of the SRP/CS and subsystems
This application example presents two safety functions:
1. Safety-related stop function initiated by a protective measure
2. Maintain interlock of the guard with motor M in motion
The safety function 1 is performed by an SRP/CS consisting of 5 subsystems (SB):
- SB11,12,13 represent the three RFID interlock devices of the NS series: SS1, SS2 and SS3
- SB14 represents the safety module CS AR-08
- SB15 represents the two contactors KM1 and KM2 in redundant architecture (cat. 4)



The safety function 2 is performed by 2 subsystems (SB):
- SB21 represents the CS AM-01 safety module for motor standstill monitoring
- SB22 represents the three NS series RFID interlock devices



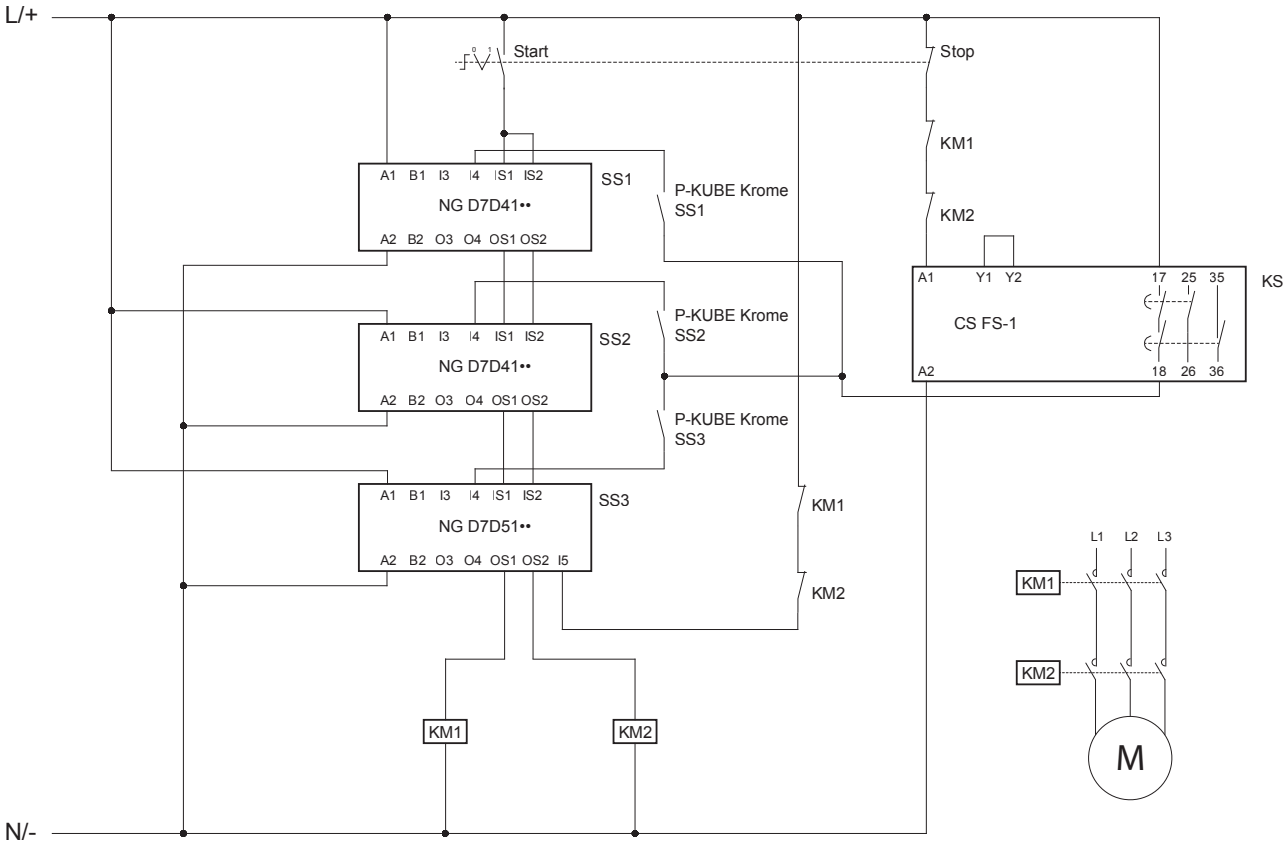
PFH_D calculation for SB15
$MTTF_D$ KM1,KM2 = 371 years.
DC = 99%, the contacts of KM1 and KM2 are monitored by the CS safety module via the feedback circuit.
For the CCF parameter we assume a score higher than 65 (acc. to EN ISO 13849-1 - Annex F).
A category 4 circuit with $MTTF_D$ = 371 and high diagnostic coverage (DC = 99%) corresponds to a failure probability of PFH_D = 6.3E-09 and a PL "e".

Calculation of the total PFH_D of the SRP/CS safety function 1
$PFH_{DTOT} = PFH_{DSB11} + PFH_{DSB12} + PFH_{DSB13} + PFH_{DSB14} + PFH_{DSB15}$ = 1E-08
It corresponds to PL "e".

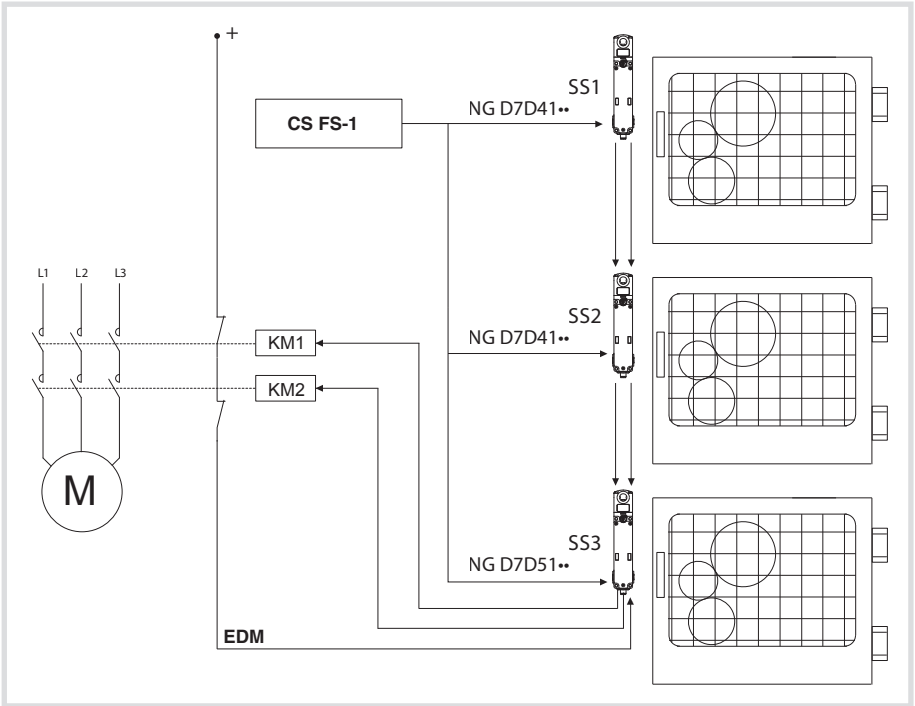
Calculation of the total PFH_D of the SRP/CS safety function 2
$PFH_{DTOT} = PFH_{DSB21} + PFH_{DSB22}$ = 8.9E-09
That would correspond to PL "e". However, considering that the motor standstill monitoring module is characterised by a PL "d", and that the unlock command takes place via a single-channel architecture, the entire SRP/CS is downgraded to this value, therefore PL "d".

Calculation example performed with SISTEMA software, downloadable free of charge at www.pizzato.com

EXAMPLE 9
Application: Guard monitoring



Reference standard EN ISO 13849-1	
Performance Level - Safety function 1	**PL e**
Performance Level - Safety function 2	**PL d**

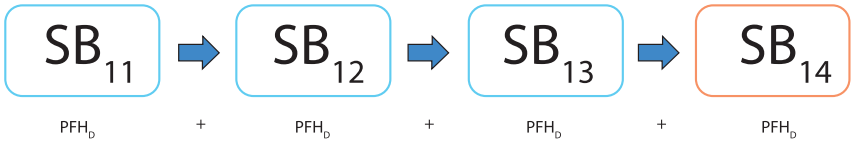


Description of the safety function
Interlocking devices SS1, SS2 and SS3 perform two safety functions: monitoring the locked state and locking the guard.
Once the guards have been released, the three sensors act directly on contactors KM1 and KM2. Contactors KM1 and KM2 (with forcibly guided contacts) are controlled by the SS3 sensor, via EDM (External Device Monitoring) input I5.
The interlock command on the three devices SS1, SS2 and SS3 depends on the closure of the safe contact of a CS FS-1 safety timer module. Each device will receive the unlock command, when the button mounted on the P-KUBE Krome handle is pressed.

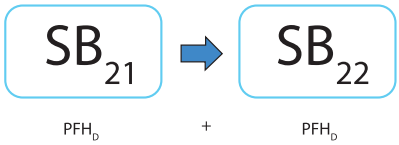
Device data
SS1, SS2, SS3 are coded interlock devices with RFID technology, with guard locking device. Locked protection detection function PFH_D = 1,17E-09 PL ="e", single channel locking control function PFH_D = 1,51E-10 PL ="d".
CS FS-1 is a safety timer module, PFH_D = 5.06E-10, PL "e".
KM1 and KM2 are contactors operated at nominal load. B10d = 1.300.000 (see EN ISO 13849-1 - Table C.1)

Assumption of the frequency of use
Each door is opened every 10 minutes, 16 hours a day, for 365 days a year, equal to nop = 35,040

Definition of the SRP/CS and subsystems
This application example presents two safety functions:
1. Safety-related stop function initiated by a protective measure
2. Maintain interlock of the guard with motor M1 in motion
The safety function 1 is performed by an SRP/CS consisting of 4 subsystems (SB):
- SB11,12,13 represent the three RFID interlock devices of the NG series: SS1, SS2 and SS3
- SB14 represents the two contactors KM1 and KM2 in redundant architecture (cat. 4)



The safety function 2 is performed by 2 subsystems (SB):



- SB21 represents the safety timer module CS FS-1
- SB22 represents the NG series RFID interlocking device

PFH_D calculation for SB14
$MTTF_D$ KM1,KM2 = 371 years.
DC = 99%, the KM1 and KM2 contacts are monitored by the last NG device in the series, via the EDM input.
For the CCF parameter we assume a score higher than 65 (acc. to EN ISO 13849-1 - Annex F).
A category 4 circuit with $MTTF_D$ = 371 and high diagnostic coverage (DC = 99%) corresponds to a failure probability of PFH_D = 6.3E-09 and a PL "e".

Calculation of the total PFH_D of the SRP/CS safety function 1
$PFH_{DTOT} = PFH_{DSB11} + PFH_{DSB12} + PFH_{DSB13} + PFH_{DSB14}$ = 9.8E-09
It corresponds to PL "e".

Calculation of the total PFH_D of the SRP/CS safety function 2
$PFH_{DTOT} = PFH_{DSB21} + PFH_{DSB22}$ = 6.6E-10
That would correspond to PL "e". Considering however, that the NG device with single channel interlock command is characterized by a PL "d", the entire SRP/CS is downgraded to this value; therefore PL "d".