

1- Foreword

Purpose of this section is to provide the machine manufacturer with a quick introduction on some standards related to machine safety, to clarify some basic principles and to provide some application examples. This brief guide refers only to the aspects related to the Functional Safety of the machine, that is all the measures aimed at protecting the machinery operator from the risks arising by their operation, and at aspects relating to the design and selection of interlock devices for guards.

It does not mention risks due to other hazards as for example electric energy presence, pressure containers, explosive atmospheres etc. which anyhow shall be evaluated by the machine manufacturer.

This document has been prepared by Pizzato Elettrica best knowledge, considering the standards and interpretations and the existent technologies in year 2015. Since some of the directives are being applied for the first time in these months it cyeart be excluded that in the meantime further directives or interpretations by the official bodies will modify the evaluations provided in this document. Therefore the examples here reported must be always evaluated by the final user according to the technology/directive progress report and they do not relieve users of their own responsibilities. Pizzato Elettrica does not take any responsibility on the reported examples and does not exclude the possibility of involuntary data errors nor inaccuracy.

2 -Design in safety. The European standards structure.

In order to be freely marketed in the countries of the European Community every device or machinery must comply with Community Directives. They establish the general principles in order for the manufacturer not to place on the market hazardous products for operators. The products and different possible hazards as a whole are very wide, that's why throughout the time many different directives have been issued. As an example we quote the low voltage directive 2006/95/EC, the explosive atmosphere directive 2014/34/UE, the electromagnetic compatibility directive 2004/108/EC, etc. Any hazard due to machinery functioning is governed by Machinery Directive 2006/42/EC.

The conformity to directives is certified by the manufacturer's issue of the Conformity Declaration and by the application of the CE marking on the machine itself.

For the risks assessment of the machine and realization of safety systems to protect the operator from those risks, the European Committees for Standardization CEN and CENELEC have issued a series of standards which translate into technical requirements the contents of directives. The standards published on the Official Journal of the European Union are to be intended as harmonized. The manufacturer who applies those standards to certify his own machineries has a presumption of conformity to the directives.

The machine safety standards are divided into three types: A, B and C.

Type A standards: give basic concepts, principles for design and general aspects that can be applied to machinery.

Type B standards: deal particularly with one or more aspects concerning the safety and they are also divided into:

- B1: standards concerning some safety aspects (e.g. safety distances, temperatures, noise, etc.)
- B2: standards concerning safety devices (e.g. two-hand controls, interlocking devices, etc.)

Type C standards: deal with detailed safety requirements for particular groups of machines (e.g. hydraulic presses, injection machineries,...).

The manufacturer of devices or machineries must first verify if the product is covered by a type C standard. If so, the standard gives the safety requirements, otherwise type B standards for any specific aspect or device of the product shall apply. Failing further requirements, the manufacturer shall follow general guidelines stated in type A standards.

TYPE A STANDARDS

for example:

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

TYPE B1 STANDARDS

for example:

EN 62061. Functional safety of safety-related electrical, electronic and programmable electronic control systems.
EN ISO 13849-1 and -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 for guards
EN 60204-1. Electrical equipment of machines
EN 60947-5-1. Electromechanical control devices.

TYPE C STANDARDS

for example:

EN 201. Machinery for rubber and plastic material - Injection machines
EN 415-1. Safety of wrapping machines
EN 692. Mechanical presses
EN 693. Hydraulic presses
EN 848-1. Safety of wood-working machines – Miller on one single side with rotating tool – Part 1: Single-shaft vertical miller (router)

3 - Designing safe machines. Risks analysis.

The first step to build a safe machine is to identify all possible hazards to which the machine operators are exposed. The hazards identification and classification allow to define the risks for the operator, that is the combination of the possibility that the hazard occurs and the type of possible injury for the operator.

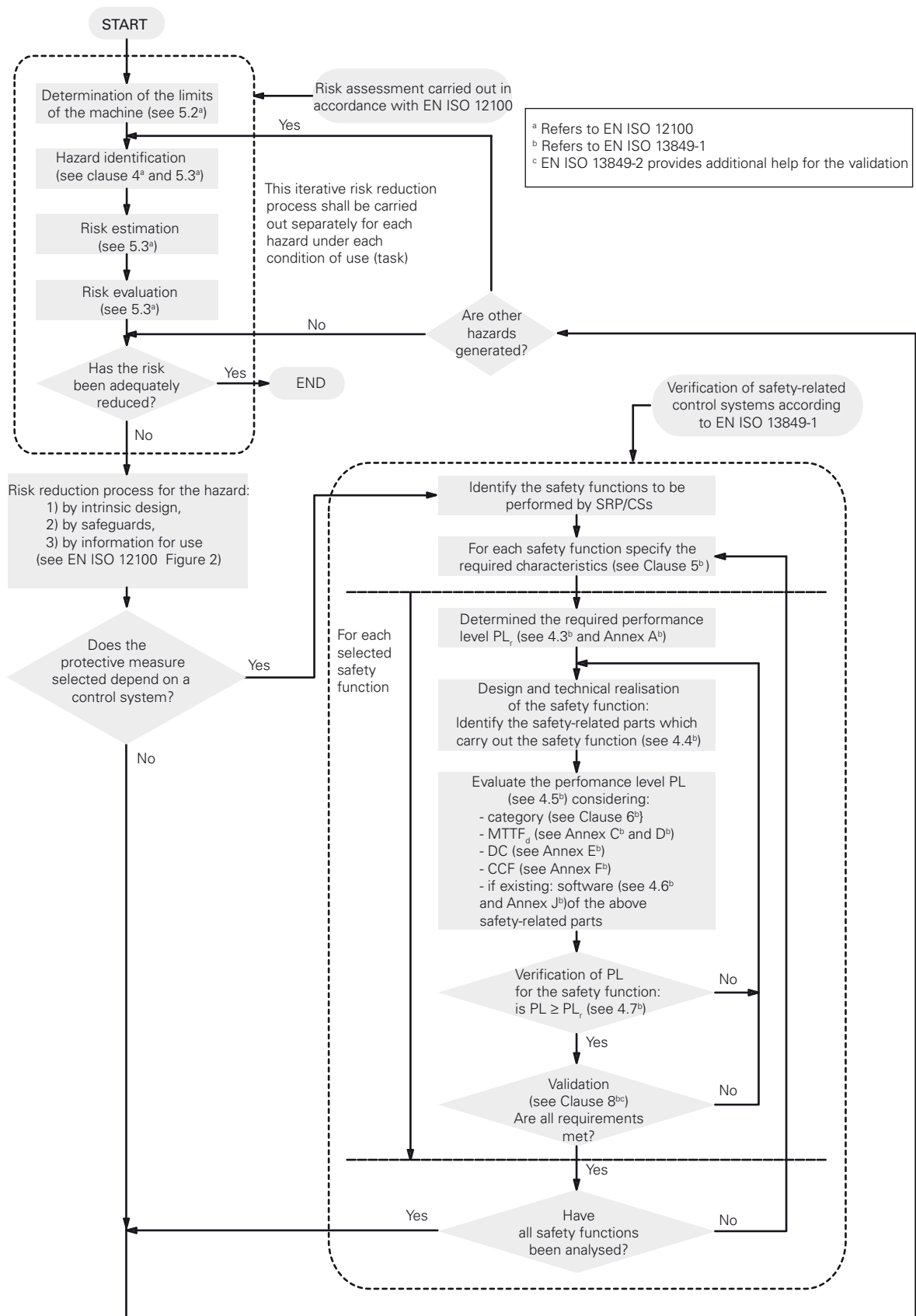
The methodology of risk analysis and assessment, of procedures for their reduction, is defined by standard EN ISO 12100. This contains a cyclic analysis model such that, once the initial objectives are agreed, the analysis of risks and possible solutions to reduce these risks are repeatedly evaluated until the objectives are met.

The model introduced by this standards provides for proceeding with the risks reduction/elimination after an analysis through a process as follows:

- 1) risks elimination at the origin, through the system structure and the use of inherently safe design principles
- 2) risks reduction by safeguarding and control systems
- 3) manifestation of residual risks by informing the users

Since each machinery presents hazards and it's not possible to completely eliminate all possible risks, the objective is to reduce the machinery risks to residual acceptable levels.

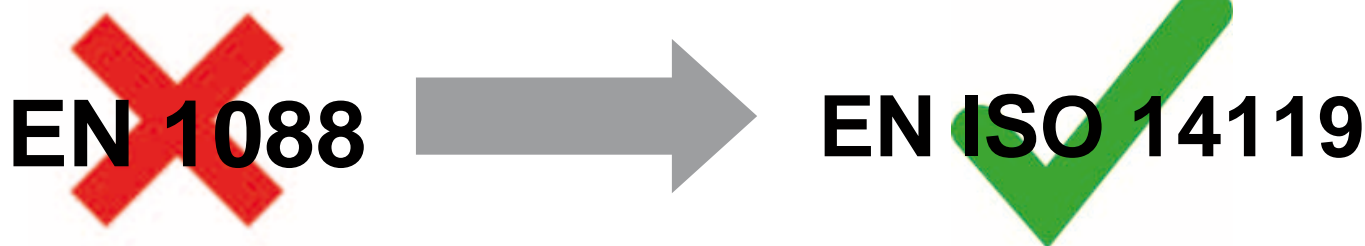
In case the risk is reduced through a control system, EN ISO 13849-1 comes into play which provides an evaluation model of the quality system. This way, for a specific level risk it's possible to use a safety function of equal or superior level.



Note: This figure has been obtained by the combination of figures 1 and 3 of EN 13849-1. The original tests are in English.

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

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



The standard involves machine designers as well as the interlock device manufacturers (and system integrators), providing requirements for the creation of the device and its correct installation.

The standard highlights some little clear aspects and considers additional technologies used for interlocking devices; defines some parameters (**actuator type and level of coding**) and regulates the specifications for correct installation, so as to increase the protection against guard manipulation.

The standard also considers other aspects related to interlocking device (e.g. guard locking principle, electromagnetic lock, auxiliary release, escape and emergency release, etc.) which are not detailed here.

Coding level of the actuators

An important change introduced by the standard is the definition of a coded actuator and the classification of the level of coding:

- **coded actuator** – actuator especially designed to actuate a specific interlocking device;
- **low level coded actuator** – actuator for which 1 to 9 variations in code are available (e.g. the magnetic sensors SR series or the safety switches with separate actuator FS, FG, FR, FD...);
- **medium level coded actuator** - actuator for which 10 to 1000 variations in code are available;
- **high level coded actuator** - actuator for which more than 1000 variations in code are available (e.g. the sensors of the SX series with RFID technology or the interlocking devices NG series with RFID technology and guard locking)

Types of interlocking devices

Standard EN ISO 14119 defines different types of interlocking devices:

- **Interlocking device type 1** - mechanical actuation by uncoded actuator (e.g. hinge interlocking devices HP series)
- **Interlocking device type 2** - mechanical actuation by coded actuator (e.g. safety switches with separate actuator of the FR, FS, FG, ... series)
- **Interlocking device type 3** - non-contact actuation by uncoded actuator
- **Interlocking device type 4** - non-contact actuation by coded actuator (e.g. RFID safety sensors ST and NG series)

Examples of actuation principle		Actuator examples		Type
Mechanical	Direct contact/force	Not encoded	Rotating cam Linear cam Hinge	Type 1
		Encoded	Key actuated Trapped key	Type 2
Without contact	Inductive	Not encoded	Ferromagnetic material	Type 3
	Magnetic		Magnet, solenoid	
	Capacitive		Any suitable object	
	Ultrasounds	Any suitable object		
Optical	Encoded	Any suitable object	Type 4	
Magnetic		Magnetically coded		
RIFD		RFID, encoded		
Optical		Optical, encoded		

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 device		Type 2 and type 4 devices (low level coded actuators)	Type 2 and type 4 devices (high level coded actuators)
	Rotary or linear cam safety switches	Hinge safety switches		
Installation out of reach (1)				
Shielding, physical obstruction (2)			X	
Installation in hidden position (3)	X			
Status monitoring or cyclic testing (4)				
Non-detachable fixing of device and actuator				
Non-detachable fixing of device		M		
Non-detachable fixing of actuator		M	M	M
Additional interlocking device and plausibility check	R		R	

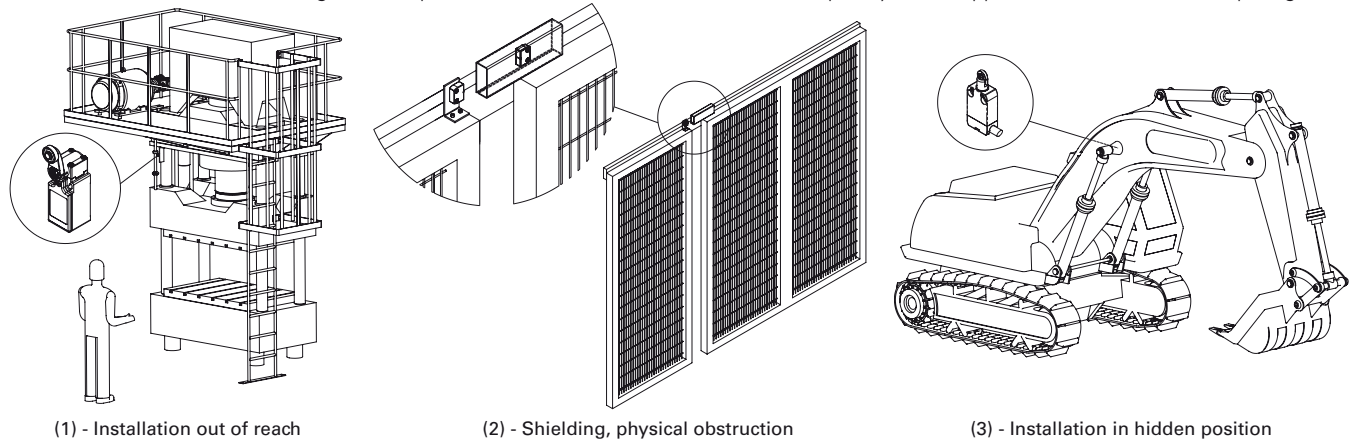
Excerpt from EN ISO 14119 - Table 3

X: obligation to apply at least one of the measures listed in the "Principles and measures to prevent circumvention" column

M: obligatory measure

R: recommended measure

It is obvious that in order to meet all the requirements of EN ISO 14119, it is easier to use devices with RFID technology with a high level of coding and hinge switches, as it is necessary to fulfil only a few requirements in order to prevent circumvention of the devices themselves. Devices with low or medium coding levels require additional measures to ensure an adequately robust application to counteract tampering.



(4) – A status monitoring can be made for example in a machine where the working cycle is easily predictable, so as to verify that at the end or during specific phases of the working cycle the guards are actually open (e.g. to remove the processed material or to make quality controls); in case the system control does not detect the guard opening actions, an alarm is generated and the machine stopped.

Guard locking devices and holding force

The manufacturer of the guard locking device shall ensure that in the engage position, the guard locking device withstands at least the specified holding force F_{zh} . This force shall be at the most equal to the maximum holding force divided by a safety coefficient equal to 1.3.

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

For example, a device with maximum specified force $F_{zh} = 2000$ N must pass a test with a maximum holding force equal to $F_{1max} = 2600$ N.

An interlocking device with guard locking shall provide both the interlocking function (guard open/closed) and the guard locking function (locked/unlocked). Each of these functions may require a different PL safety level (ref. EN ISO 13849-1). In most cases the PL of the guard locking function is lower than the PL of the interlocking function. (See paragraph 8.4, note 2 of EN ISO 14119).

To highlight that an interlocking device provides also the locking monitoring, the new standard requires that the product shall have the symbol represented aside.



5 - Normative present situation. Reason of changes, new standards and some overlapping

“Traditional” standards for Functional Safety as EN 954-1 had the great merit of formalizing some of the basic principles in the safety circuits analysis in accordance to deterministic principles. On the other hand they don't deal with programmable electronic devices at all, and generally they suffer the passed time. To include the programmable electronic devices in the control system analysis, the new standards approach is basically probabilistic therefore new statistical variables have been introduced.

This approach original standard is the IEC 61508 which deals the safety of complex programmable electronic systems. It's an impressive standard (divided in 8 sections for a total amount of almost 500 pages) suitable for different application fields (process industry, industrial machineries, nuclear plants), so that it has achieved the status of type A standard (not harmonized). The standard introduces the SIL concept (Safety Integrity Level) that is a probabilistic indication of a system residual risk.

From IEC 61508 comes EN 62061, which in particular concerns safety in industrial machineries complex and programmable electronic systems. The concepts introduced by this standard allow the application generally to any control system with electric, electronic and programmable electronic technology (excluding non-electric technology systems).

EN ISO 13849, developed by CEN under ISO aegis, also comes from this probabilistic approach but it tries to make the manufacturer used to the EN 954-1 concepts pass to the new concepts in a less traumatic way. The standard is applied to electromechanical, hydraulic, not complex electronic systems and to some programmable electronic systems with predefined structures. EN ISO 13849 is a type B1 standard, it introduces the PL concept (Performance Level) that is, as for SIL, a probabilistic indication of machinery residual risk. In this standard it is indicated a correlation between SIL and PL; there are concepts borrowed by EN 61508 (as DC and CCF) and it is established a reference with safety categories of EN 954-1.

In the functional safety field for control circuits safety, there are presently two standards in force (year 2013):

- EN ISO 13849-1. Type B1 standard which uses the PL concept.
- EN 62061. Type B1 standard which uses the SIL. concept.

The two standards EN 62061 and EN ISO 13849-1 show a discrete overlapping concerning the application field. For several aspects they are alike and there's a precise link between the two different symbols (SIL and PL) which indicates the two standards analysis result.

The recommendation on the two standards application ambit is stated in EN ISO 13849-1, table 1 and, as you can see, both standards can be applied for wide products typologies.

PL EN ISO 13849-1	a	b	c	d	e	
SIL EN 62061 - IEC 61508	-	1	2	3	(4)	
PFH _d	10 ⁻⁴	10 ⁻⁵	3x10 ⁻⁶	10 ⁻⁶	10 ⁻⁷	10 ⁻⁸
A hazardous failure every n years	~1	~10	~40	~100	~1000	~10000

Important note.

EN 13849-1 is a type B1 standard, therefore if a machinery is already classified by a type C standard is this last one to prevail. All type C standards previously developed are based on concepts of EN 954-1. For manufacturers of machineries covered by a type C standard, the introduction time of new standards could be different according to the updating speed of the various technical committees.

Table 1 - Recommended application of EN 62061 and EN ISO 13849-1

	Technology used by the part of the control system that is linked to safety	EN ISO 13849-1	EN 62061
A	Not electrical, hydraulic for example	X	Not handled
B	Electromechanical, for example relays and/ or non-complex electronics	Limited to designated architectures ^a and up to PL=e	All architectures up to SIL 3
C	Complex electronics, for example programmable	Limited to designated architectures ^a and up to PL=d	All architectures up to SIL 3
D	A combined with B	Limited to designated architectures ^a and up to PL=e	X ^c
E	C combined with B	Limited to designated architectures (see note 1) and up to PL=d	All architectures up to SIL 3
F	C combined with A or C combined with A and B	X ^b	X ^c

X indicates that the line is covered by the international standard shown in the head of the column

a. Designated architectures are defined in clause 6.2 (EN ISO 13849-1) to provide a simplified approach to quantification of the performance level

b. For complex electronics: the designated architectures are used according to this part of EN ISO 13849-1 and up to PL=d, or any architecture which is compliant with EN 62061

c. For non-electrical technologies, the parts are used as subsystems in accordance with this part of EN ISO 13849-1

Note. Taken from table 1 of EN ISO 13849-1:2006

The choice of the standard to be used is up to the manufacturer according to the adopted technology. We believe that EN ISO 13849-1 is a standard easier to apply thanks to its mediate approach and reutilization of the concepts already known to the market.

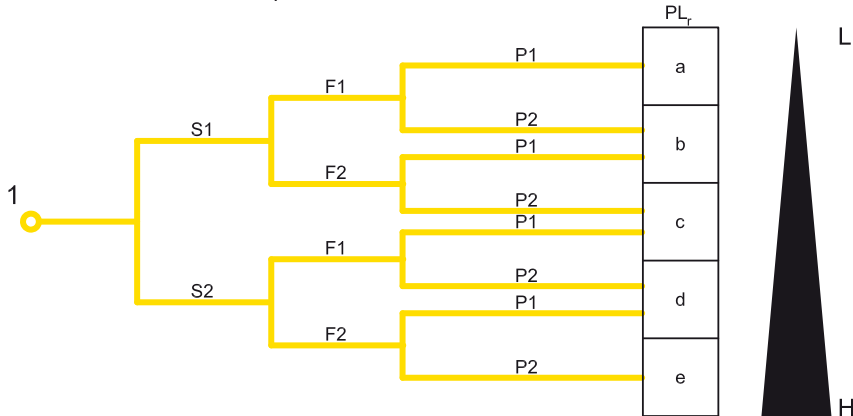
Note: In 2008 the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA) has introduced a report (BGIA Report 2/2008) on the EN ISO 13849-1 application where it is stated that the recommendations and restrictions for EN ISO 13849-1 applications must be considered obsolete, therefore even in case of programmable electronics (case C and E in the above table) the limit can be considered PL e.

6- EN ISO 13849-1 and new parameters: PL, MTTF_d, DC, CCF

EN ISO 13849-1 provides the manufacturer with an iterative method to assess if a machine risk can be limited to an acceptable residual risk through adequate safety functions. The adopted method provides for each risk an hypothesis-analysis-validation cycle at the end of which it must be demonstrated that every intended safety function is adequate to the related risk being considered.

The first step consists in the evaluation of the Performance Level required by each safety function. The first step consists in the evaluation of the Performance Level required by each safety function. As for EN 954-1, also EN 13849 uses a graph for a machine function risk analysis (figure A.1) determining, instead of a required safety category, a Required Performance level or PL_r for the safety function which protects that machine part. The machinery manufacturer, starting from the graph point 1 and answering to S, F and P questions, will identify the PL_r for the intended safety function. The manufacturer then shall make a system to protect the machinery operator with a PL performance level equal or greater than the required.

Risk graph for determining required PL_r for safety function (taken by EN 13849-1, figure A.1)



Key

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

Risk parameters

- S** Severity of injury
 - S1** slight (normally reversible injury)
 - S2** serious (normally irreversible injury or death)
- F** Frequency and/or exposure to hazard
 - F1** seldom-to-less-often and/or exposure time is short
 - F2** frequent-to-continuous and/or exposure time is long
- P** Possibility of avoiding hazard or limiting harm
 - P1** possible under specific conditions
 - P2** scarcely possible

Note: It would be easier for a manufacturer not having to repeat the machine risk analysis and try to use the data already derived from an EN 954-1 risk analysis.

Generally this is not possible since with the new standard the risk graph changed (see figure above) therefore, with identical risks, the required safety function levels can have changed. The German Institute BGIA in its report 2008/2 on EN ISO 13849-1 suggests that a conversion could be adopted through a worst-case approach as in the following table. For further information refer to the mentioned report.

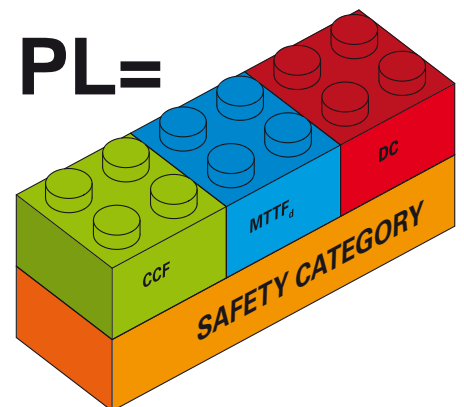
Category requested by EN 954-1	Performance requested (PL _r) and Category requested acc. to EN ISO 13849-1
B	→ b
1	→ c
2	→ d, Category 2
3	→ d, Category 3
4	→ e, Category 4

Five performance levels are set out, from PL_a to PL_e on risk increasing and each one of them identifies a numerical range of average probability of dangerous failure per hour. For example PL_d defines that the average probability of a dangerous failure per hour is included between 1x10⁻⁶ and 1x10⁻⁷, that is about 1 dangerous failure every 100-1000 years.

PL	Average probability of dangerous failure per hour PFHd (1/h)	
a	≥ 10 ⁻⁵	e < 10 ⁻⁴
b	≥ 3 x 10 ⁻⁶	e < 10 ⁻⁵
c	≥ 10 ⁻⁶	e < 3 x 10 ⁻⁶
d	≥ 10 ⁻⁷	e < 10 ⁻⁶
e	≥ 10 ⁻⁸	e < 10 ⁻⁷

Other measures are also necessary to achieve the PL of a control system, which are:

1. The system Safety Category which derives from the architecture (structure) of the control system and its behaviour under fault conditions
2. MTTF_d of components
3. DC or system Diagnostic Coverage.
4. CCF or system Common Cause Failure.





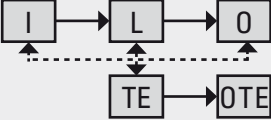
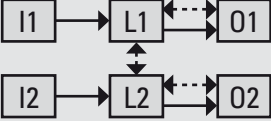
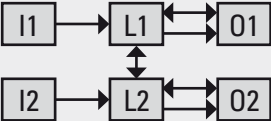
Safety Categories.

The majority of control circuits normally used are represented by a logic block structure:

- Input or signals input
- Logic or processing signals logic
- Output or control signals output

differently combined according to the control circuit structure.

EN ISO 13849-1 allows for five different basic circuit structures termed Designated Architectures. These architectures, combined with the fault-mode behaviour and some minimum values of $MTTF_d$, DC and CCF, indicate the system control Safety Category as shown in the following table. EN ISO 13849-1 Safety Categories therefore are not the same but they extend the Safety Category concept introduced by the previous EN 954-1.

Category	Summary of requirements	System behaviour	Principles used to achieve safety	$MTTF_d$ of each channel	DC_{avg}	CCF
B	Safety-related parts of control systems and/or their protective equipment, as well as their components, shall be designed, constructed, selected, assembled and combined in accordance with relevant standards so that they can withstand the expected influences. Basic safety principles shall be used. Architecture: 	The occurrence of a fault can lead to the loss of the safety function.	Mainly characterized by selection of components	Low or Medium	None	Not relevant
1	Requirements of category B shall apply. Well-ried components and well-ried safety principles shall be used. Architecture: 	The occurrence of a fault can lead to the loss of the safety function but the probability of occurrence is lower than for Category B.	Mainly characterized by selection of components	High	None	Not relevant
2	Requirements of category B and the use of well-ried safety principles shall apply. Safety function shall be checked at suitable intervals by the machine control system. Architecture: 	The occurrence of a fault can lead to the loss of the safety function between the checks. The loss of the safety function is detected by the check.	Mainly characterized by structure	Low to High	Low to Medium	See Annex F
3	Requirements of category B and the use of well-ried safety principles shall apply. Safety-related parts shall be designed so that: – a single fault in any of these parts does not lead to the loss of the safety function, and – whenever reasonably practicable, the single fault is detected. Architecture: 	When a single fault occurs the safety function is always performed. Some, but not all faults will be detected. Accumulation of undetected faults can lead to the loss of the safety function.	Mainly characterized by structure	Low to High	Low to Medium	See Annex F
4	Requirements of category B and the use of well-ried safety principles shall apply. Safety-related parts shall be designed, so that: – a single fault in any of these parts does not lead to a loss of the safety function, and – a single fault is detected at or before the next demand upon the safety function. If this is not possible, then the accumulation of undetected faults must not lead to the loss of the safety function. Architecture: 	When a single fault occurs the safety function is always performed. Detection of accumulated faults reduces the probability of the loss of the safety function (high DC). The faults will be detected in time to prevent the loss of the safety function.	Mainly characterized by structure	High	High (including accumulation of faults)	See Annex F

MTTF_d ("Mean Time To Dangerous Failure";).

This parameter tries to determine the system component "safety quality" by defining its mean lifetime before a dangerous failure (note that it is not a generic failure) stated in years. Practically, the calculation of the MTTF_d is based on numerical values supplied by the components manufacturers. Where there's a lack of data the standard itself lists some typical values in specific reference tables (EN ISO 13849-1 Annex C). The calculation leads to a numerical value included in 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

In case of wearable components (typically mechanic and hydraulic devices), instead of the component MTTF_d, the manufacturer shall provide the component B_{10d} data that is the average number of the component operations until 10% of the units studied have failed dangerously. The component B_{10d} has to be converted to MTTF_d by the machine manufacturer with the formula:

$$MTTF_d = \frac{B_{10d}}{0,1 \cdot n_{op}}$$

Where n_{op} = component mean number of annual operations.

Assuming the machine daily operating frequency and the daily operating hours, n_{op} can be determined from:

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

where

d_{op} = operating time in days per year

h_{op} = operating time in hours (h) per day

t_{ciclo} = cycle time (s)

Note that the MTTF_d parameter, when it derives from a wearable component, does not depend only from the component itself but also from the application. A electromechanical device with low operating frequency, e.g. a contactor only used for emergency stop, generally has a high MTTF_d but if the same device is used for normal cycle operation here the contactor MTTF_d, with low cycle time, can drop dramatically.

All the control circuit single components are used to calculate the circuit MTTF_d according to its structure. In one channel architecture circuits (as in category B, 1 and 2) every single components contribution is linear and the channel MTTF_d calculation is determined from:

$$\frac{1}{MTTF_d} = \sum_{i=1}^N \frac{1}{MTTF_{di}}$$

In order to avoid too optimistic interpretation the maximum MTTF_d value of each channel is restrained to 100 years. No channel with MTTF_d inferior to 3 years is allowed.

In case of two channel systems (categories 3 and 4) the circuit MTTF_d calculation is determined from symmetrically arranging the two channels MTTF_d 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 tries to indicate the effectiveness of a system' self-test monitoring its possible failures. According to the percentage of dangerous failures detectable by the system the diagnostic coverage shall be different. The DC parameter is a percentage value which is estimated by some values stated in a table (EN ISO 13849-1 annex E) according to the measures adopted by the manufacturer to detect any anomaly in its circuit. Since, in general, there are different measures to detect different anomalies in the same circuit, the average value or DC_{avg} calculation results in four levels, which are:

High DC_{avg} ≥ 99%

Medium 90% ≤ DC_{avg} < 99%

Low 60% ≤ DC_{avg} < 90%

None DC_{avg} < 60%

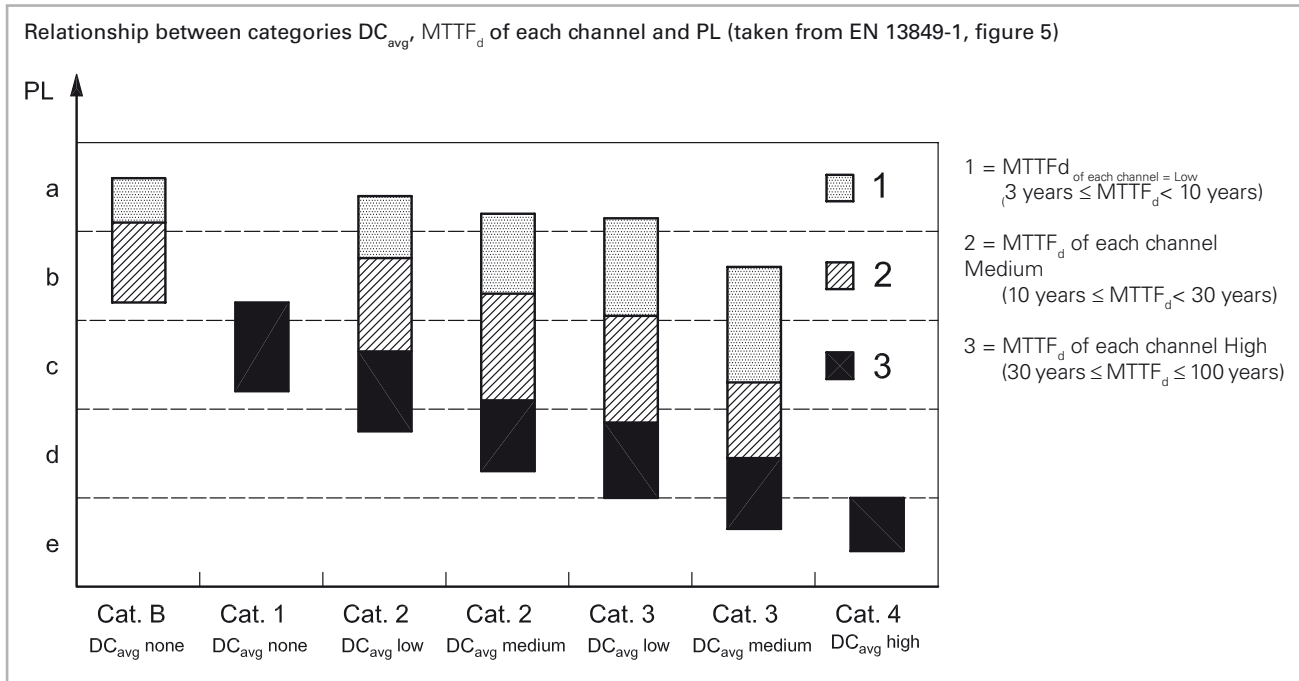
The None diagnostic coverage is admitted only for systems with architecture B or 1.

CCF ("Common Cause Failures")

Only in case of category 2, 3 or 4 systems for the calculation of PL it is necessary also the evaluation of possible common cause failure or CCF that can invalidate the systems redundancy. The evaluation is made by a check-list (EN ISO 13849-1 Annex F) which determines points from 0 to 100 according to the adopted solutions against common cause failures. The minimum value admitted for categories 2,3 and 4 is 65 points.

PL ("Performance Level")

Knowing all this data, EN ISO 13849-1 determines the system PL by a correlation table (EN ISO 13849-1 Annex K) or by a simplified graphic figure (EN ISO 13849-1 paragraph 4.5) as follows.



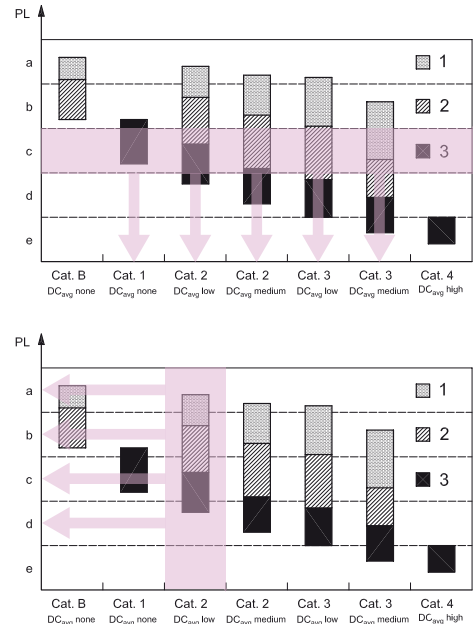
This image is very useful since it can be read from different point of view. Given a certain PL_r , the graph shows all the different solutions which determine that PL, that is the possible circuit structures which provide the same PL.

For instance, observing the figure, to obtain a system having a PL equal to "c" level all the following solutions are possible:

1. Category 3 system with little affordable components ($MTTF_d$ =low) and medium DC.
2. Category 3 system with affordable components ($MTTF_d$ =medium) and low DC.
3. Category 2 system with affordable components ($MTTF_d$ =medium) and medium DC.
4. Category 2 system with affordable components ($MTTF_d$ =medium) and low DC.
5. Category 1 system with highly affordable components ($MTTF_d$ =high).

At the same time the figure, chosen a circuit structure, allows to immediately see the max. PL reachable according to the average diagnostic coverage and the components $MTTF_d$. Therefore the manufacturer can exclude at once some circuit structures because not adequate to the required PL_r .

In general though, to identify the system PL do not refer to this figure since in many cases the graphic areas superimpose on the different PL margin lines. Instead, the table in EN ISO 13849-1 Annex K can be used for a precise determination of the circuit PL.



Safety parameters table

The B10d data shown in the table refer to the mechanical life of the device contacts, under normal ambient conditions. NO contacts may be used within the safety circuit only if combined with an NC contact, and must be monitored (for example, by a PLC or safety module). The value in B10d for NC and NO contacts refers to a maximum electrical load equal to 10% of the current value shown in the application category. Mission time (for all items indicated below): 20 years.

Electromechanical 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 and solenoid	1,000,000	5,000,000	20%
FS	Safety switches with separate actuator with lock and solenoid	1,000,000	4,000,000	20%
F•••96 F•••95	Safety switch with pin for hinge	1,000,000	5,000,000	20%
F•••C•	Switches with slotted hole lever for swing 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 (used with compatible Pizzato Elettrica safety modules)	20,000,000	20,000,000	50%
SR	Magnetic safety sensors (used at max. load: DC12 24 V 250 mA)	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	Prewired modular 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} (NC)	B ₁₀ /B _{10d}
E2 1PU1•••••••	Single maintained buttons	2,000,000	50%
E2 1PU2•••••••	Single spring-return buttons	30,000,000	50%
E2 1PD•••••••, E2 1PT•••••••	Double and triple buttons	2,000,000	50%
E2 1PE•••••••	Emergency buttons	600,000	50%
E2 1SE•••••••, E2 1SL•••••••	Selector switches and illuminated selector switches	2,000,000	50%
E2 1SC•••••••	Selector switches with key	600,000	50%
E2 1PQ•••••••	Quadruple buttons	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 pin for hinge	500,000	2,500,000	20%
F•••C•-EX•	Switches with slotted hole lever for swing guards	500,000	1,000,000	50%
F•••••-EX•	Rope switches for emergency stop	500,000	1,000,000	50%

Electronic devices

Code	Article description	MTTF _d	DC	PFH _d	SIL CL	PL	Cat
HX BEE1-•••	Safety hinge with electronic unit	4018	H	2.29E-11	3	e	4
ST	Safety sensors with RFID technology	4077	H	1.46E-09	3	e	4
NG	RFID safety switches with lock	1883	H	8.07 E-10	3	e	4
CS AM-01	Standstill monitor safety module	145	M	1.94E-09	2	d	3
CS AR-01, CS AR-02	Safety module for monitoring of guards and emergency stops	227	H	1.18E-10	3	e	4
CS AR-04	Safety module for monitoring of guards, emergency stops	152	H	1.84E-10	3	e	4
CS AR-05, CS AR-06	Safety module for monitoring of guards, emergency stops and light barriers	152	H	1.84E-10	3	e	4
CS AR-07	Safety module for monitoring of guards and emergency stops	111	H	7.56E-10	3	e	4
CS AR-08	Safety module for monitoring of guards, emergency stops and light barriers	218	H	4.58E-10	3	e	4
CS AR-20, CS AR-21	Safety module for monitoring of guards and emergency stops	225	H	4.18E-10	3	e	3
CS AR-22, CS AR-23	Safety module for monitoring of guards and emergency stops	151	H	5.28E-10	3	e	3
CS AR-24, CS AR-25	Safety module for monitoring of guards and emergency stops	113	H	6.62E-10	3	e	3
CS AR-40, CS AR-41	Safety module for monitoring of guards and emergency stops	225	H	4.18E-10	2	d	2
CS AR-46	Safety module for monitoring of guards and emergency stops	435	-	3.32E-08	1	c	1
CS AR-51	Safety module for monitoring of safety mats and bumpers	209	H	9.43E-09	3	e	4
CS AR-90	Safety module for monitoring of lift floor leveling	382	H	5.03E-10	3	e	4
CS AR-91	Safety module for monitoring of lift floor leveling	227	H	1.18E-10	3	e	4

B_{10d}: Number of operations before 10% of the components have failed dangerously
 B₁₀: Number of operations before 10% of the components have failed
 B₁₀/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	Article description	MTTF _d	DC	PFH _d	SIL CL	PL	Cat
CS AR-93	Safety module for monitoring of lift floor leveling	227	H	1.34E-10	3	e	4
CS AR-94	Safety module for monitoring of lift floor leveling	213	H	5.62E-09	3	e	4
CS AR-94•U12	Safety module for monitoring of lift floor leveling	227	H	1.13E-10	3	e	4
CS AR-95	Safety module for monitoring of lift floor leveling	213	H	5.42E-09	3	e	4
CS AT-0•, CS AT-1•	Safety module with timer for monitoring of guards and emergency stops	84	H	9.01E-09	3	e	4
CS AT-3•	Safety module with timer for monitoring of guards and emergency stops	74	H	4.05E-09	3	e	4
CS DM-01	Safety module for monitoring of two-hand controls	142	H	2.99E-08	3	e	4
CS DM-02	Safety module for monitoring of two-hand controls	206	H	2.98E-08	3	e	4
CS DM-20	Safety module for monitoring of two-hand controls	42	-	1.32E-06	1	c	1
CS FS-1•	Safety timer module	146	H	1.62E-09	3	e	4
CS FS-2•, CS FS-3•	Safety timer module	205	M	1.10E-08	2	d	3
CS FS-5•	Safety timer module	349	M	1.17E-08	2	d	3
CS ME-01	Contact expansion module	76	H	6.38E-10	①	①	①
CS ME-02	Contact expansion module	113	H	2.84E-09	①	①	①
CS ME-03	Contact expansion module	208	M	2.45 E-08	①	①	①
CS ME-20	Contact expansion module	113	H	3.07E-09	①	①	①
CS ME-3•	Contact expansion module	112	H	2.77E-09	①	①	①
CS M•201	Multifunctional safety module	133	H	4.54E-10	3	e	4
CS M•202	Multifunctional safety module	573	H	4.73E-10	3	e	4
CS M•203	Multifunctional safety module	101	H	5.74E-10	3	e	4
CS M•204	Multifunctional safety module	132	H	5.32E-10	3	e	4
CS M•205	Multifunctional safety module	406	H	4.83E-10	3	e	4
CS M•206	Multifunctional safety module	643	H	2.85E-10	3	e	4
CS M•207	Multifunctional safety module	407	H	5.39E-09	3	e	4
CS M•208	Multifunctional safety module	588	H	6.17E-09	3	e	4
CS M•301	Multifunctional safety module	126	H	8.92E-10	3	e	4
CS M•302	Multifunctional safety module	604	H	3.45E-10	3	e	4
CS M•303	Multifunctional safety module	459	H	9.11E-10	3	e	4
CS M•304	Multifunctional safety module	97	H	1.01E-09	3	e	4
CS M•305	Multifunctional safety module	503	H	7.24E-10	3	e	4
CS M•306	Multifunctional safety module	99	H	8.25E-10	3	e	4
CS M•307	Multifunctional safety module	276	H	5.84E-09	3	e	4
CS M•308	Multifunctional safety module	514	H	6.42E-09	3	e	4
CS M•309	Multifunctional safety module	469	H	6.61E-09	3	e	4
CS M•401	Multifunctional safety module	413	H	1.16E-09	3	e	4
CS M•402	Multifunctional safety module	452	H	6.67E-09	3	e	4
CS M•403	Multifunctional safety module	416	H	6.86E-09	3	e	4

B_{10d}: Number of operations before 10% of the components have failed dangerously
 B₁₀: Number of operations before 10% of the components have failed
 B₁₀/B_{10d}: ratio of total failures to dangerous failures.
 MTTF_d: Mean Time To Dangerous Failure

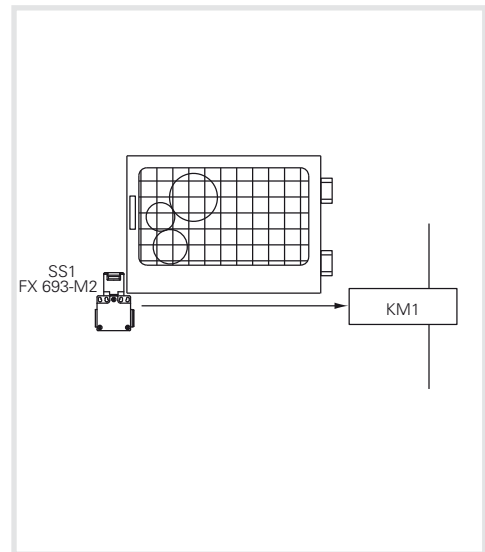
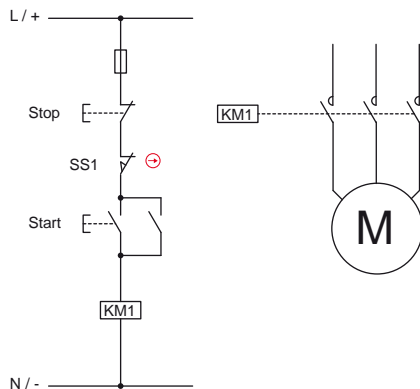
DC: Diagnostic Coverage
 PFH_d: Probability of Dangerous Failure per hour
 SIL CL: Safety Integrity Level Claim Limit. Maximum achievable SIL according to EN 62061
 PL: Performance Level. PL acc. to EN ISO 13849-1

① Dependent from the base module

EXAMPLE 1**Application: Guard monitoring**

Reference standard EN ISO 13849-1

Safety category	1
Performance Level	PL c



The control circuit in the figure has a guard monitoring function. If the guard is open the engine must not start. The hazards analysis points out how the system does not have inertia, that is the engine, once de-energizing the power, stops faster than opening the guard. The risk analysis shows the required PL_r target is PL c. It is necessary to verify if the assumed control system, which has a one channel structure, has a PL higher or equal to PL_r .

Description of the safety function

The guard position is detected by the switch with separate actuator SS1 which operates directly on the contactor KM1. The contactor KM1 that controls the moving parts is usually activated by the buttons Start and Stop but the working cycle analysis shows that also the guard is open at every operation cycle. Consequently, the contactor and the switch number of operation can be considered equal.

The circuit structure is one channel type without supervision (category B or 1) where there are only Input (switch) and Output (contactor) components.

The safety function is not performed when a device failure occurs.

No measures for fault detection are implemented.

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 tested device according to EN ISO 13849-2 table D.4. The device B_{10d} value is supplied by the manufacturer (see page 271) equal to 2,000,000 operations.
- KM1 is a contactor used at nominal value. It's a well tested device in accordance with EN ISO 13849-2 table D.4. Its B_{10d} value is equal to 2,000,000 operations. This value is determined from the standard tables (see EN ISO 13849-1 table C.1).

Assumption of the frequency of use

- It is assumed that the machinery is used for 365 days per year, for three shifts of 8 hours and 600 s cycle time. Therefore the operations per year both for the contactor and the switch is equal to maximum $N_{op} = (365 \times 24 \times 3,600) / 600 = 52,560$.
- An operation of the start button every 300 seconds is assumed. The annual operations are at maximum equal to $n_{op}/year = 105,120$
- KM1 contactor shall be actuated both for the machine normal start-stop and the restart after the guard opening. $n_{op}/year = 52,560 + 105,120 = 157,680$

MTTF_d Calculation

The $MTTF_d$ of the SS1 switch is equal to: $MTTF_d = B_{10d} / (0,1 \times n_{op}) = 2000000 / (0,1 \times 52560) = 381$ years

The $MTTF_d$ of the KM1 contactor is equal to: $MTTF_d = B_{10d} / (0,1 \times n_{op}) = 2000000 / (0,1 \times 157680) = 127$ years

In consequence the one channel circuit $MTTF_d$ is equal to: $1 / (1/381 + 1/127) = 95$ years

Diagnostic Coverage DC_{avg}

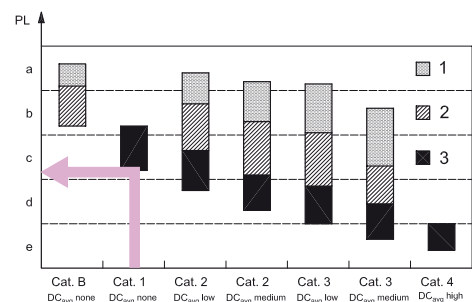
No measures for fault detection are implemented therefore the diagnostic coverage is None, admitted condition for the considered circuit which is in category 1.

CCF Common Cause Failure

No CCF calculation is necessary for a category 1 circuit.

PL verification

From the standard table or figure 5 we can verify that for a Category 1 circuit with $MTTF_d = 95$ years the resulting PL of the control circuit is PL c. Therefore the PL_r target is reached.



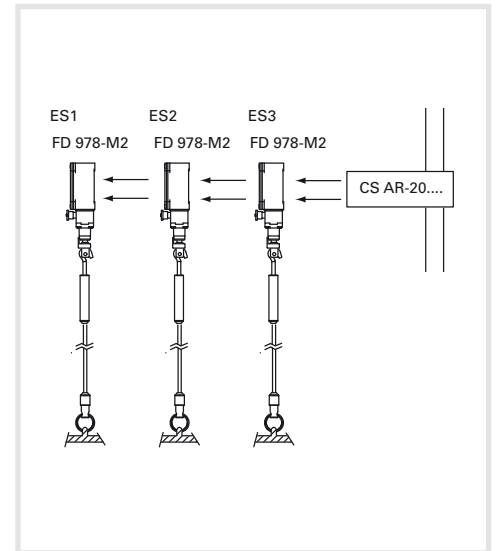
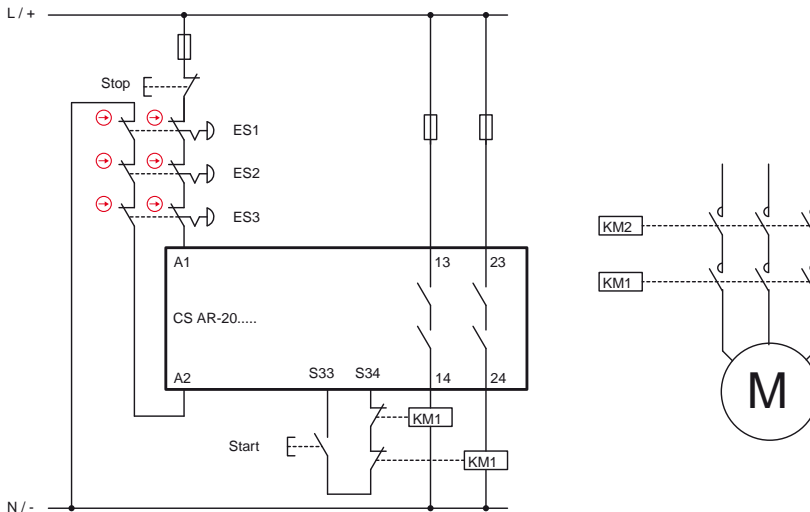
EXAMPLE 2**Application: Emergency stop control**

Reference standard EN ISO 13849-1

Safety category

3

Performance Level

PL e**Description of the safety function**

The operation of one emergency device causes the safety module and the two contactors KM1 and KM2 to intervene.

The ES1, ES2, ES3 device signal is redundantly read by the CS safety module. Also the KM1 and KM2 contactors (with forcibly guided contacts) are monitored by CS via the feedback circuit.

Device data:

- ES1, ES2, ES3 (FD 978-M2) are rope switches for emergency stop with positive opening. The B_{10d} value is equal to 2,000,000 (see page 271)
- KM1, KM2 are contactors used at nominal load. The device B_{10d} value is equal to 2,000,000 (see EN ISO 13849-1 Table C.1)
- CS is a safety module (CS AR-20) with $MTTF_d=225$ years (see page 271) and DC= High
- The circuit architecture is two channels type in category 3

Assumption of the frequency of use

- Twice a month $n_{op}/year = 24$
- Start button operation: 4 times a day
- Assuming 365 working day, contactors shall intervene $4 \times 365 + 24 = 1,484$ times/year
- Switches are operated with the same frequency.
- The case of more buttons pushed together is not considered.

MTTF_d Calculation

- $MTTF_{d,ES1,ES2,ES3} = 833.333$ years
- $MTTF_{d,KM1,KM2} = 13.477$ years
- $MTTF_{d,CS} = 225$ years
- $MTTF_{d,CH1} = 221$ years. Value restricted to 100 years. The channels are symmetric thus $MTTF_d=100$ years (High)

Diagnostic Coverage DC_{avg}

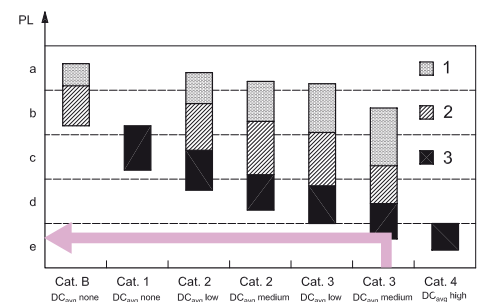
- KM1 and KM2 contactors are monitored by CS via the feedback circuit. DC=99% (High)
- The CS AR-20 safety module has a High diagnostic coverage.
- Not all faults in the emergency device series can be detected. The diagnostic coverage is 90% (Medium)

CCF Common Cause Failure

We assume a score > 65 (based on EN ISO 13849-1 - annex F).

PL verification

- A category 3 circuit with $MTTF_d=High$ and $DC_{avg}=High$ can reach a PL e.



Any information or application example, included the connection diagrams, described in this document are to be intended as purely descriptive. The choice and application of the products in conformity with the standards, in order to avoid damage to persons or goods, is the user's responsibility.

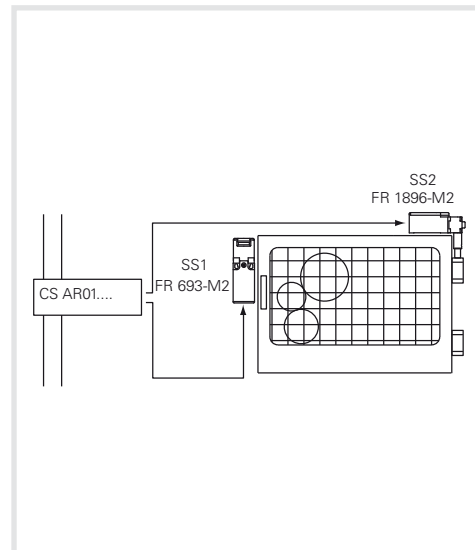
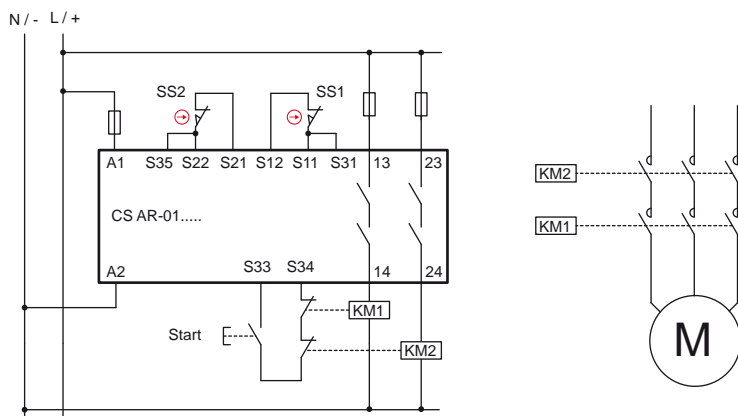
EXAMPLE 3**Application: Guard monitoring**

Reference standard EN ISO 13849-1

Safety category

4

Performance Level

PL e**Description of the safety function**

The guard opening causes the SS1 and SS2 switches to intervene; consequently the safety module and the KM1 and KM2 contactors do the same.

The SS1, SS2 device signal is redundantly monitored by the CS safety module.

The switches have a different operating principle.

Also the KM1 and KM2 contactors (with forcibly guided contacts) are monitored by CS via the feedback circuit.

Device data:

- SS1 (FR 693-M2) is a switch with positive opening. The B_{10d} value is equal to 2,000,000 (see page 271)
- SS2 (FR 1896-M2) is a hinge operating switch with positive opening. $B_{10d} = 5.000.000$ (see page 271)
- KM1, KM2 are contactors used at nominal load. $B_{10d} = 2,000,000$ (see EN ISO 13849-1 - Table C.1)
- CS is a safety module (CS AR-01) with $MTTF_d = 227$ years and DC= High

Assumption of the frequency of use

365 days/year, 16 h/day, 1 operation every 4 minutes (240 s). $n_{op}/year = 87,600$

MTTF_d Calculation

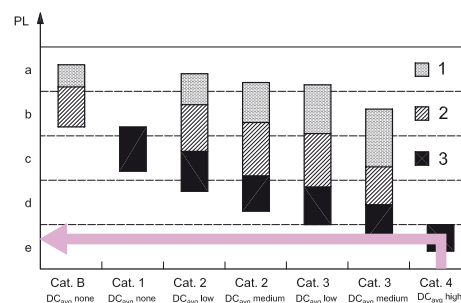
- $MTTF_{d, SS1} = 228$ years
- $MTTF_{d, SS2} = 571$ years
- $MTTF_{d, KM1, KM2} = 228$ years
- $MTTF_{d, CS} = 227$ years
- $MTTF_{d, CH1} = 67$ years (SS1, CS, KM1)
- $MTTF_{d, CH2} = 77$ years (SS2, CS, KM2)
- $MTTF_d$: symmetrically arranging the two channels, the result is $MTTF_d = 72.1$ years (High)

Diagnostic Coverage DC_{avg}

- SS1, SS2 have DC=99% since SS1, SS2 contacts are monitored by the CS and they have different operating principles.
- KM1 and KM2 contactors are monitored by CS via the feedback circuit. DC=99% (High)
- The CS AR-01 has an internal redundant and self-monitoring circuit. DC = High
- $DC_{avg} = High$

PL verification

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



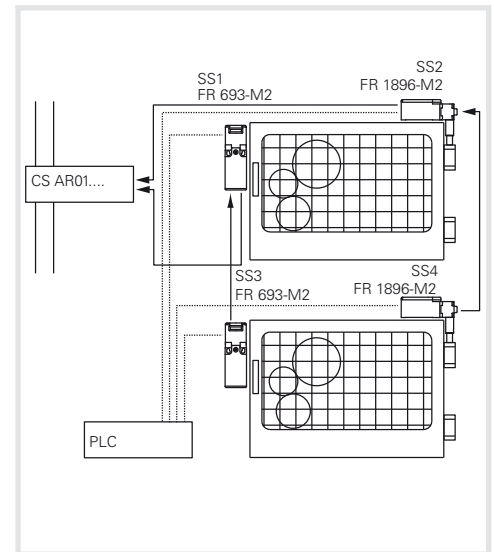
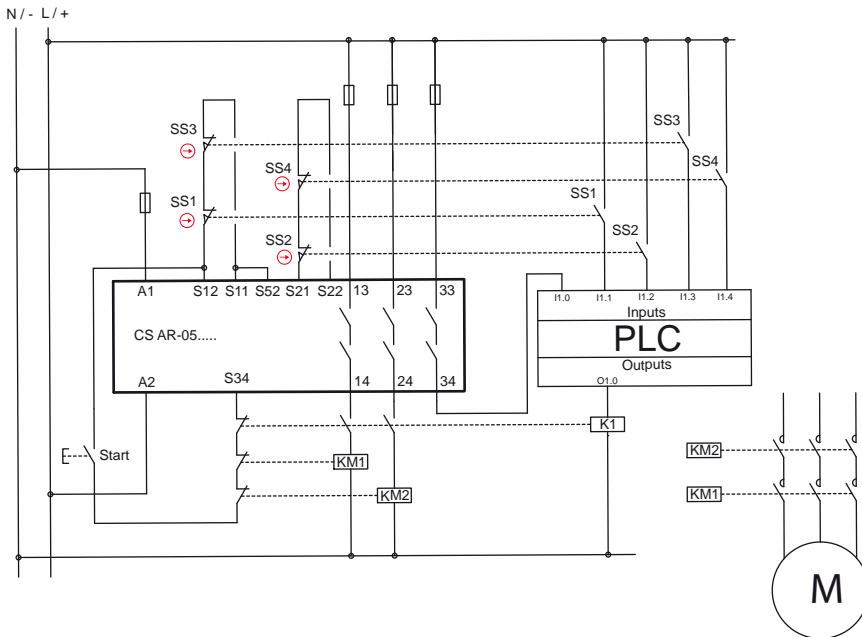
EXAMPLE 4**Application: Guard monitoring**

Reference standard EN ISO 13849-1

Safety category

4

Performance Level

PL e**Description of the safety function**

The opening of a guard causes the SS1, SS2 switches to intervene on the first guard and SS3, SS4 on the second; the switches trigger the safety module and the KM1 and KM2 contactors.

The SS1, SS2 and SS3, SS4 device signal is redundantly monitored by the CS safety module, furthermore the switch auxiliary contact is monitored by PLC.

The switches have a different operating principle.

Also the KM1 and KM2 contactors (with forcibly guided contacts) are monitored by CS via the feedback circuit.

Device data:

- SS1, SS3 (FR 693-M2) are switches with positive opening. The B_{10d} value is equal to 2,000,000 (see page 271)
- SS2, SS4 (FR 1896-M2) is a hinge operating switch with positive opening. $B_{10d} = 5.000.000$ (see page 271)
- KM1, KM2 are contactors used at nominal load. The device B_{10d} value is equal to 2,000,000 (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 and 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
- $MTTF_{d, KM1, KM2} = 285$ years
- $MTTF_{d, CS} = 152$ years
- $MTTF_{d, Ch1} = 84$ years (SS1, CS, KM1) / (SS3, CS, KM1)
- $MTTF_{d, Ch2} = 93$ years (SS2, CS, KM2) / (SS4, CS, KM2)
- $MTTF_d$: symmetrically arranging the two channels, the result is $MTTF_d = 88.6$ years (High).

Diagnostic Coverage DC_{avg}

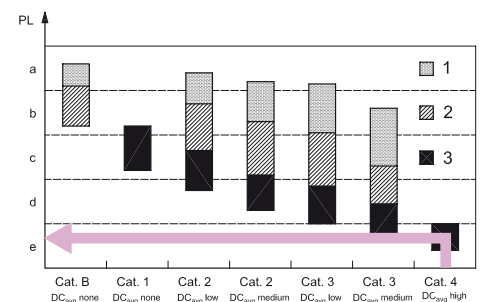
- KM1, KM2 contacts are monitored by CS via the feedback circuit. DC=99%
- All auxiliary contacts of the switches are monitored by PLC. DC=99%
- The CS AR-05 module has a DC= High (see page 271)
- The diagnostic coverage for both channels is 99% (High)

CCF Common Cause Failure

- We assume a score > 65 (based on EN ISO 13849-1 - annex F).

PL verification

- A category 4 circuit with $MTTF_d = 88.6$ years (High) and $DC_{avg} = \text{High}$ corresponds to a PL e.



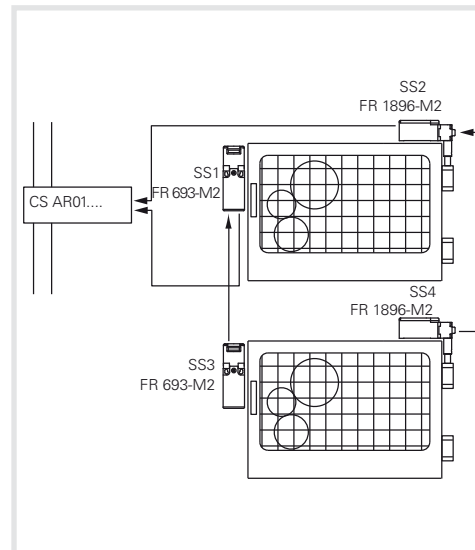
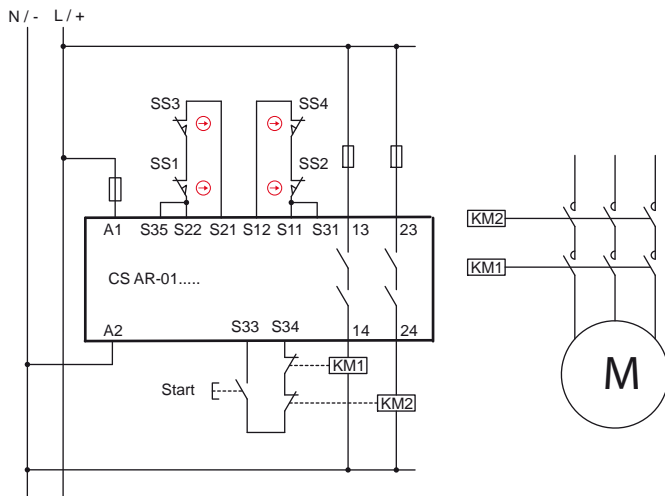
EXAMPLE 5**Application: Guard monitoring**

Reference standard EN ISO 13849-1

Safety category

3

Performance Level

PL e**Description of the safety function**

The opening of a guard causes the SS1, SS2 switches to intervene on the first guard and SS3, SS4 on the second; the switches trigger the safety module and the KM1 and KM2 contactors.

The SS1, SS2 and SS3, SS4 device signal is redundantly monitored by the CS safety module.

The switches have a different operating principle.

Also the KM1 and KM2 contactors (with forcibly guided contacts) are monitored by CS via the feedback circuit.

Device data:

- SS1, SS3 (FR 693-M2) are switches with positive opening. The B_{10d} value is equal to 2,000,000 (see page 271)
- SS2, SS4 (FR 1896-M2) is a hinge operating switch with positive opening. $B_{10d} = 5.000.000$ (see page 271)
- KM1, KM2 are contactors used at nominal load. The device B_{10d} value is equal to 2,000,000 (see EN ISO 13849-1 table C.1)
- CS is a safety module (CS AR-01) with $MTTF_d = 227$ years and DC= High

Assumption of the frequency of use

- 2 times per hour for 16 h/day and 365 days/year equal to $n_{op}/year = 11,680$
- The contactors will operate for twice the number of operations = 23,360

MTTF_d Calculation

- $MTTF_{d, SS1, SS3} = 1,712$ years
- $MTTF_{d, SS2, SS4} = 4,281$ years
- $MTTF_{d, KM1, KM2} = 856$ years
- $MTTF_{d, CS} = 227$ years
- $MTTF_{d, CH1} = 162$ years (SS1, CS, KM1) / (SS3, CS, KM1)
- $MTTF_{d, CH2} = 172$ years (SS2, CS, KM2) / (SS4, CS, KM2)
- $MTTF_{d} =$ value restricted to 100 years

Diagnostic Coverage DC_{avg}

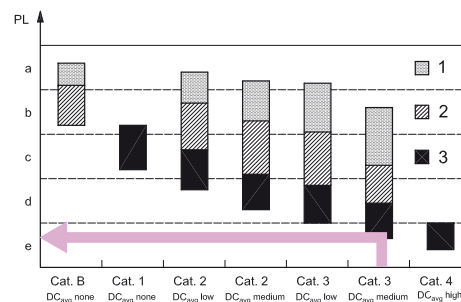
- KM1, KM2 contacts are monitored by CS via the feedback circuit. DC=99%
- Not all faults in the switch series can be detected. DC=60%
- The CS AR-01 module has a DC= High
- We assume a diagnostic coverage of 92% (Medium)

CCF Common Cause Failure

- We assume a score > 65 (based on EN ISO 13849-1 - annex F).

PL verification

- A category 3 circuit with $MTTF_d = 100$ years and $DC_{avg} =$ medium corresponds to a PL e.

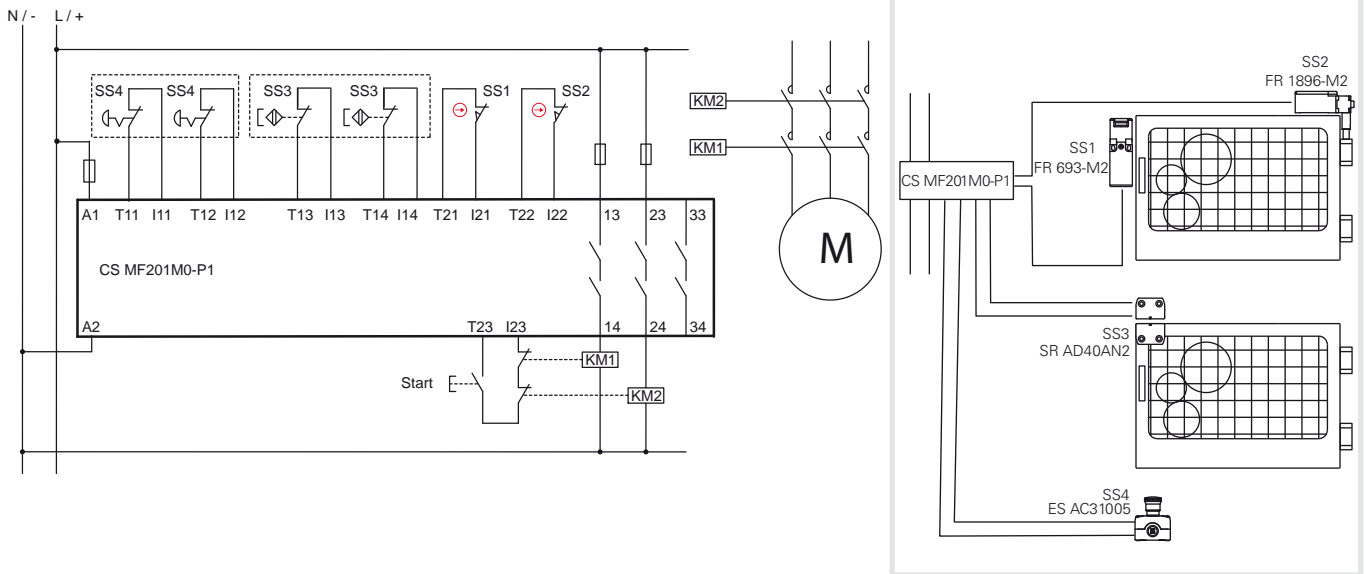


EXAMPLE 6

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 causes the SS1, SS2 switches to intervene on the first guard and SS3 sensor on the second; the switches trigger the safety module and the KM1 and KM2 contactors.

The SS1, SS2 and SS3 device signals are redundantly monitored by the CS MF safety module.

There is also an emergency button, which is also connected with a double channel to the safety module.

Also the KM1 and KM2 contactors (with forcibly guided contacts) are monitored by CS MF via the feedback circuit.

Device data:

- SS1 (FR 693-M2) is a switch with positive opening. $B_{10d} = 2,000,000$ (see page 271)
- SS3 (FR 1896-M2) is a hinge operating switch with positive opening. $B_{10d} = 5,000,000$ (see page 271)
- SS3 (SR AD40AN2) is a magnetic safety sensor. $B_{10d} = 20,000,000$ (see page 271)
- SS4 (ES AC31005) is a box with emergency button (E2 1PERZ4531) with two NC contacts. $B_{10d} = 600,000$ (see page 271)
- KM1, KM2 are contactors used at nominal load. $B_{10d} = 2,000,000$ (see Table C.1 of EN ISO 13849-1)
- CS MF201M0-P1 is a safety module with $MTTF_d = 842$ years and $DC = 99\%$

Assumption of the frequency of use

- Each gate is opened 2 times per hour for 16 h/day and 365 days/year equal to $n_{op}/year = 11,680$
- It is assumed that the emergency pushbutton is actuated at most 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
- $MTTF_d KM1, KM2 = 843$ years
- $MTTF_d CS = 842$ years
- $MTTF_d CH1 = 338$ years (SS1, CS, KM1)
- $MTTF_d CH2 = 383$ years (SS2, CS, KM2)
- $MTTF_d =$ value restricted to 100 years

Guard SS3

- $MTTF_d SS3 = 17,123$ years
- $MTTF_d KM1, KM2 = 843$ years
- $MTTF_d CS = 842$ years
- $MTTF_d = 411$ years
- $MTTF_d =$ value restricted to 100 years

Emergency button SS4

- $MTTF_d SS4 = 16,438$ years
- $MTTF_d KM1, KM2 = 843$ years
- $MTTF_d CS = 842$ years
- $MTTF_d = 410$ years
- $MTTF_d =$ value restricted to 100 years

Diagnostic Coverage DC_{avg}

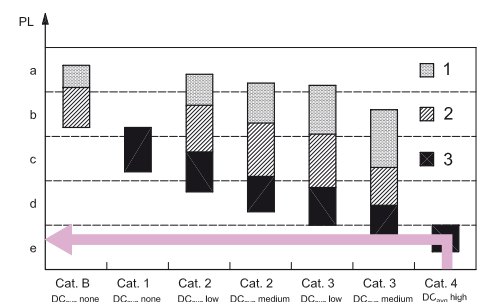
- KM1, KM2 contacts are monitored by CS MF via the feedback circuit. $DC = 99\%$
- All faults in the device series SS1, SS2 and SS3 can be detected. $DC = 99\%$
- The CS MF201M0-P1 module has a $DC = 99\%$
- We assume a diagnostic coverage of 99% (High)

CCF Common Cause Failure

- We assume a score > 65 (based on EN ISO 13849-1 - annex F).

PL verification

- A category 4 circuit with $MTTF_d = 100$ years and $DC_{avg} =$ High corresponds to a PL e.
- The safety functions connected to guards SS1/SS2, SS3 and to the button have PL e.



Any information or application example, included the connection diagrams, described in this document are to be intended as purely descriptive. The choice and application of the products in conformity with the standards, in order to avoid damage to persons or goods, is the user's responsibility.

EXAMPLE 7

Application: Guard monitoring

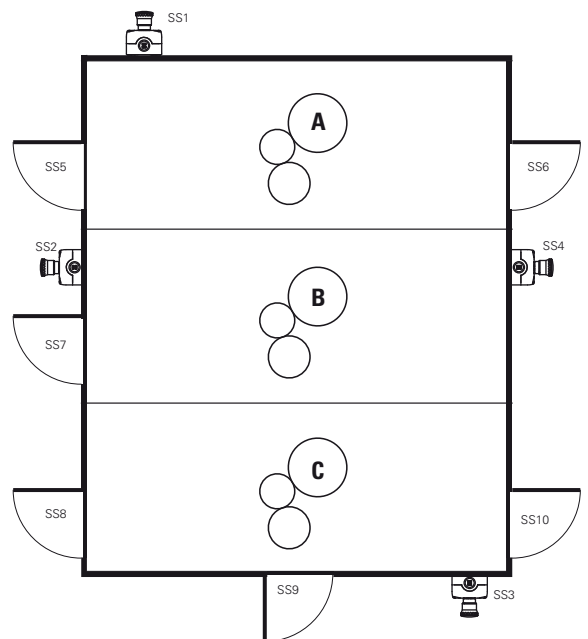
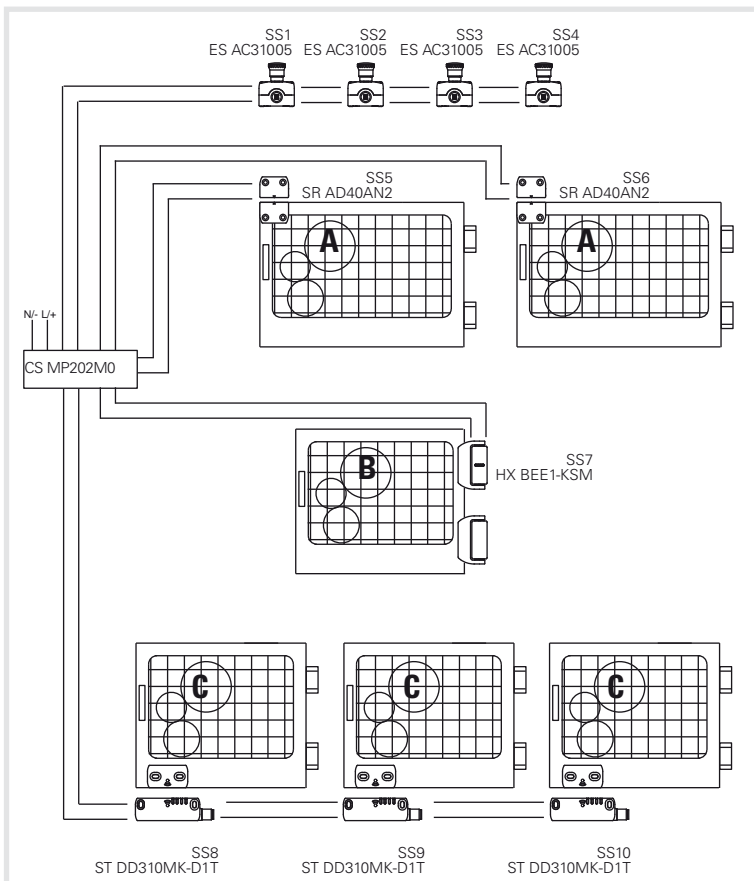
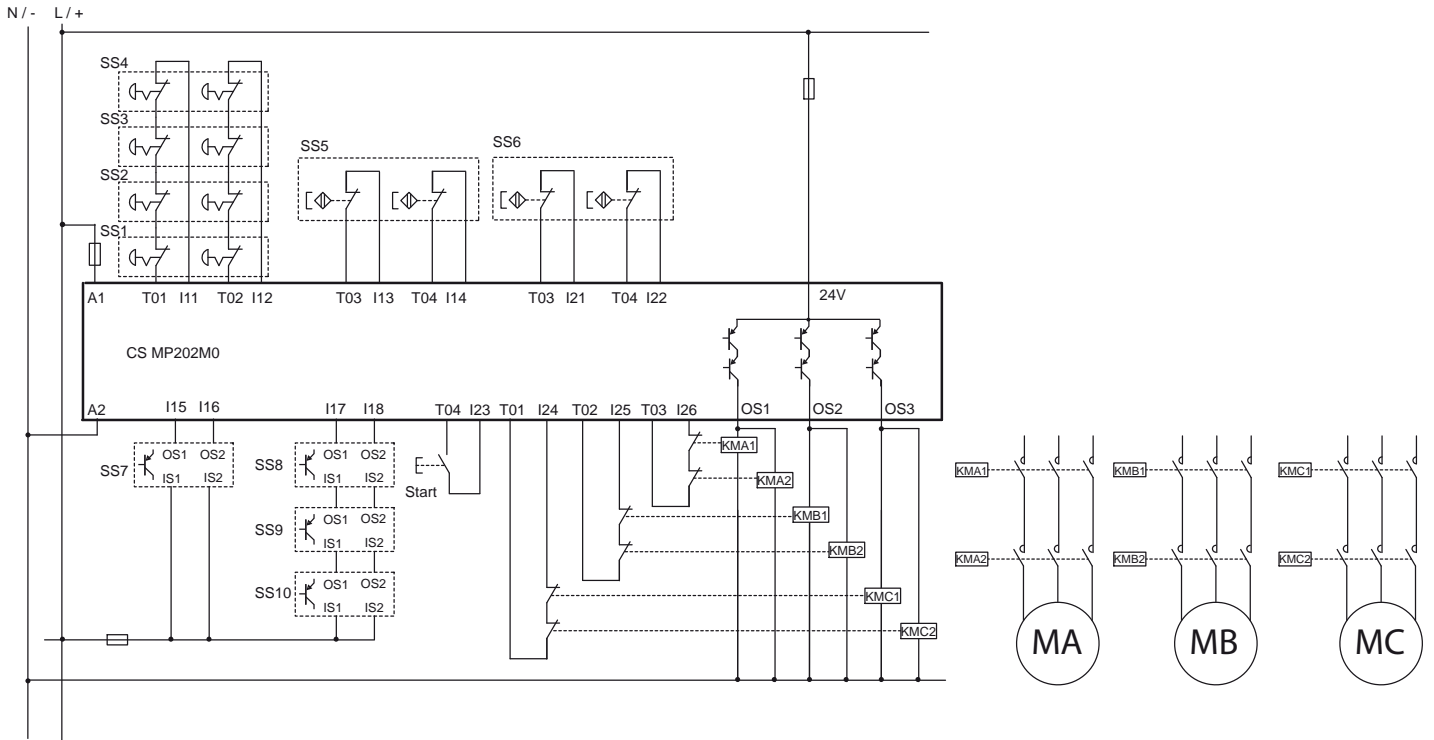
Reference standard EN ISO 13849-1

Safety category

4

Performance Level

PL e



Description of the safety function

The machine is divided into 3 different zones: access to each area is controlled by guards, and there is a series of 4 emergency buttons. When activating the emergency button, the CS MP safety module and the forcibly guided contactors KMA1/2, KMB1/2, KMC1/2 stop all motors.

The opening of a guard in zone A causes the intervention of device SS5 or SS6, which triggers the CS MP safety module and contactors KMA1 and KMA2, thus stopping the MA motor. Devices SS5, SS6 are connected separately and with a double channel to the CS MP safety module. The opening of the guard in zone B causes the intervention of SS7, which triggers the CS MP safety module and the two contactors KMB1 and KMB2, thus stopping the MB motor. The SS7 hinge has two OSSD outputs and is controlled redundantly by the CS MP safety module.

The opening of a guard in zone C causes the intervention of device SS8, SS9 or SS10, which triggers the safety module and the two contactors KMC1 and KMC2, thus stopping the MC motor. Sensors SS8, SS9 and SS10 are connected to each other via to the OSSD outputs, and are redundantly controlled by the CS MP safety module.

Device data

- SS1, SS2, SS3 and SS4 (ES AC31005) are emergency buttons (E2 1PERZ4531) with 2 NC contacts. $B_{10d} = 600,000$ (see page 271)
- SS5 and SS6 (SR AD40AN2) are magnetic safety sensors. $B_{10d} = 20,000,000$ (see page 271)
- SS7 (HX BEE1-KSM) is a safety hinge with OSSD outputs. $MTTF_d = 4077$ years / DC=99% (see page 271)
- SS8, SS9 and SS10 (ST DD310MK-D1T) are safety sensors with RFID technology and OSSD outputs. $MTTF_d = 4077$ years / DC=99% (see page 271)
- KMA, KMB and KMC are contactors used at nominal load. $B_{10d} = 2,000,000$ (see Table C.1 of EN ISO 13849-1)
- CS MP202M0 is a safety module with $MTTF_d = 2035$ years / DC=99%

Assumption of the frequency of use

- Each zone A gate is opened 2 times per hour for 16 h/day and 365 days/year equal to $n_{op}/year = 11,680$. The contactors will operate for twice the number of operations = 23,360
- Zone B gate is opened 4 times per hour for 16 h/day and 365 days/year equal to $n_{op}/year = 23,360$. The contactors will operate for a given number of operations = 23,360
- Each zone C gate is opened once per hour for 16 h/day and 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 pushbutton is actuated at most once a week, $n_{op}/year = 52$
- Fault exclusion: it is hypothesized that the pairs of contactors connected in parallel to the respective safety outputs are permanently cabled inside the electrical panel; therefore, the possibility of short circuit between +24V and contactors is excluded. (see Table D.4, D.5.2 of EN ISO 13849-2).

MTTF_d Calculation

Emergency buttons

- $MTTF_d$ SS1/SS2/SS3/SS4 = 115,384 years
- $MTTF_d$ CS = 2035 years
- $MTTF_d$ KMC1, KMC2 = 1141 years
- $MTTF_d$ e-stop = 727 years, value restricted to 100 years

Zone A guards

- $MTTF_d$ SS5/SS6 = 17.123 years
- $MTTF_d$ CS = 2035 years
- $MTTF_d$ KMA1, KMA2 = 856 years
- $MTTF_d$ A = 582 years (SS5/SS6, CS, KMA), value restricted to 100 years

Zone B gate

- $MTTF_d$ SS7 = 4.077 years
- $MTTF_d$ CS = 2035 years
- $MTTF_d$ KMB1, KMB2 = 856 years
- $MTTF_d$ B = 525 years (SS7, CS, KMB), value restricted to 100 years

Zone C guards

- $MTTF_d$ SS8/SS9/SS10 = 4.077 years
- $MTTF_d$ CS = 2035 years
- $MTTF_d$ KMC1, KMC2 = 1141 years
- $MTTF_d$ C = 620 years (SS8/SS9/SS10, CS, KMC), value restricted to 100 years

Diagnostic Coverage DC_{avg}

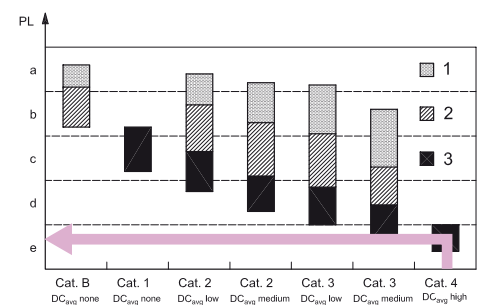
- KMA, KMB e KMC contacts are monitored by CS MP via the feedback circuit. DC=99%
- All faults of the various devices can be detected. DC=99%
- CS MP202M0 module has a DC=99%
- For each function we assume a diagnostic coverage of 99%

CCF Common Cause Failure

- We assume a score > 65 for all safety functions (based on EN ISO 13849-1 annex F).

PL verification

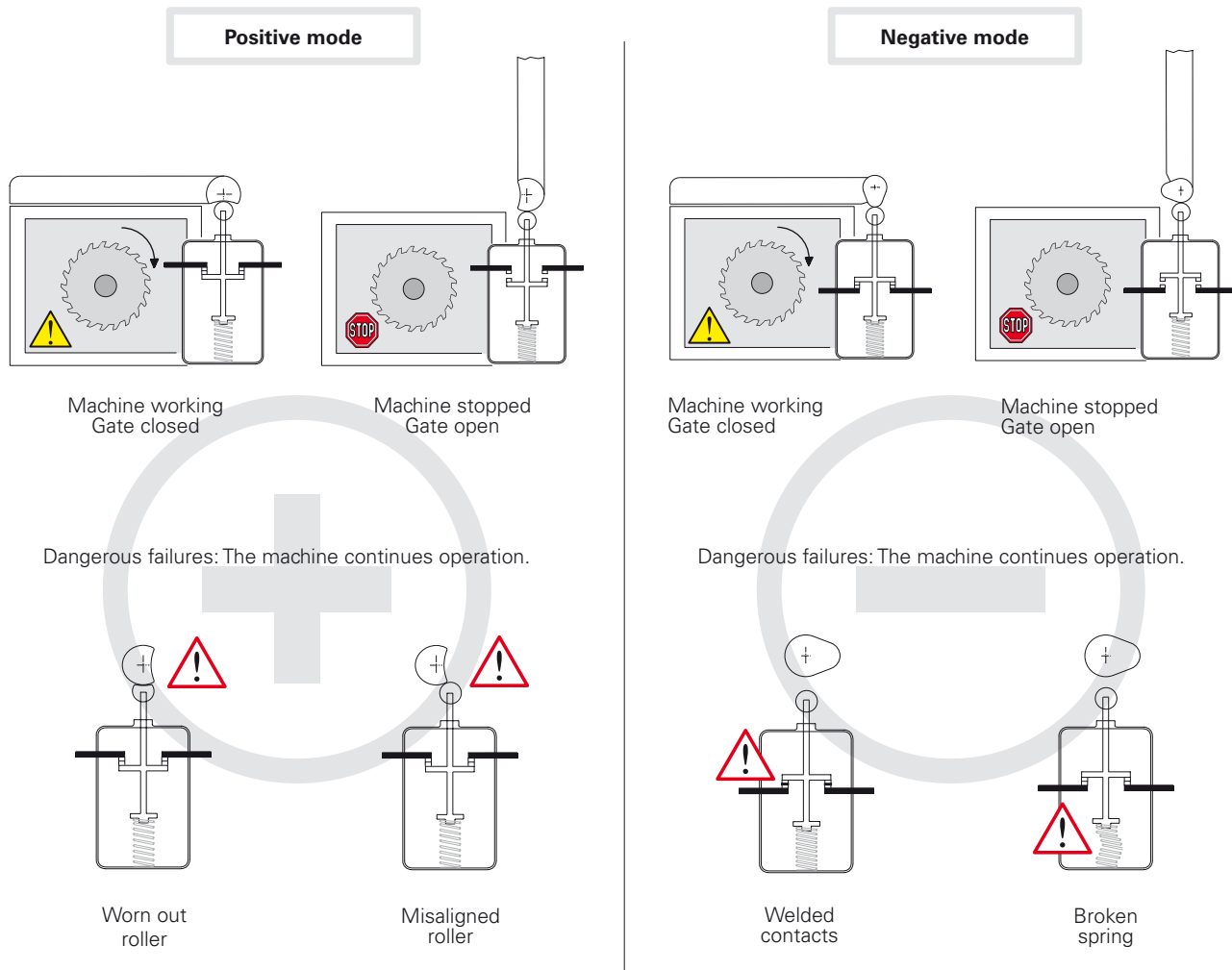
- A category 4 circuit with $MTTF_d = 100$ years and $DC_{avg} = \text{High}$ corresponds to a PL e.
- All safety functions for the guards and the emergency buttons have PL e.



7 - Positive opening, redundancy, diversification and self-control

Positive mode and negative mode.

According to the standard EN ISO 12100, if a mechanical component in motion, directly drives another component, through physical contact or a rigid mechanical linkage, that connection is said to be in a **positive manner**. 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.) their connection is in a **negative manner**.




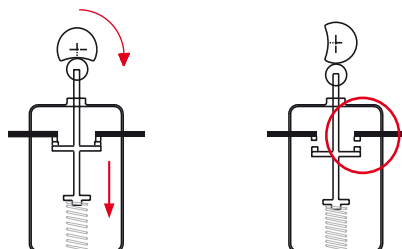
The positive mode avoids, with preventive maintenance, the dangerous failures indicated above. In negative mode, on the contrary, failures occur inside the switch and are therefore difficult to be detected.

With positive mode, internal failures (welded contacts or broken springs) allow the opening of the contacts and therefore the stop of the machine.



Use of switches in safety applications

When a single switch is used in a safety function, it must be actuated in a positive manner. The opening contact (normally closed), must be with “**positive opening**” in order to be used for safety applications. All switches with the symbol  are provided with NC contacts with positive opening.



Rigid non-flexible connection between the moving contacts and the actuator, where the actuating force is applied.

If the switches are two or more, it is suggested that they should operate in opposite modes, for example:

- One with a normally closed contact (opening contact) actuated by the guard in positive mode.
- The other with a normally open contact (closing contact), actuated by the guard in negative mode.

This is a common practice, however, it does not exclude, if justified, the use of two switches actuated in a positive mode (see diversification).

Diversification

Safety in the redundant system is increased by **diversification**. It is obtained by the application of two limit switches with different design and/or technology, in order to avoid failures caused by the same reasons. Some examples of diversification are: the use of a switch working in positive manner together with one working in non-positive manner; a switch with mechanical actuation and one with non mechanical actuation (e.g. electronic sensor); two switches with mechanical actuator working in positive manner but with different actuation principles (e.g. one actuator operated FR 693-M2 and one hinge operated FR 1896-M2 switch).

Redundancy

The **Redundancy** is the use of more than one device or system in order to guarantee that, in case of a function failure in one of them, another one is available to perform the safety functions. If the first failure is not detected, an eventual second failure may cause the loss of the safety functions.

Self-monitoring

The **Self-monitoring** consists in the automatic checking of the right function of every device running in the machine working-cycle. Consequently, the next working cycle can be either accepted or rejected.

Redundancy and self-monitoring

The combination of both systems, **redundancy** and **self-monitoring** allows that a first failure in the safety circuit does not cause the loss of safety functions. This first failure will be detected at the next re-start or anyhow before a second failure, which may cause the loss of the safety functions.