

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 machine Functional Safety, that is all the measures aiming to protect the machineries operator from their working risks. 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 2011. Since some of the directives are being applied for the first time in these months it cannot 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 94/9/EC, 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

EN ISO 12100-1 and -2:2010 (replaces EN 292-1 and EN 292-2). Basic concepts, general principles for design.
EN 61508. Functional safety of electrical, electronic, electronic programmable safety-related systems.
EN ISO 14121:2007: Principles of risk assessment.
.....

TYPE B1 STANDARDS

EN 62061:2005 Functional safety of safety-related electrical, electronic and programmable electronic control systems.
EN ISO 13849-1:2006 and -2:2003 Safety-related parts of control systems.
.....

TYPE B2 STANDARDS

EN 574:2008 Two-hand control devices.
EN 13580:2006 (replaces EN 418:1992) Emergency stop
EN 1088:2008 and ISO 14119 Interlocking devices associated with guards.
EN 60204-1:2006 Electrical equipment of machines
EN 60947-5-1:2009 Electromechanical control devices.
.....

TYPE C STANDARDS

EN 201:2007 Machinery for rubber and plastic material - Injection machines
EN 415-1.-7:2009. Safety of wrapping machines
EN 692:2009 Mechanical presses
EN 693:2009 Hydraulic presses
EN 848-1:2010 Safety of wood-working machines – Miller on one single side with rotating tool – 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.

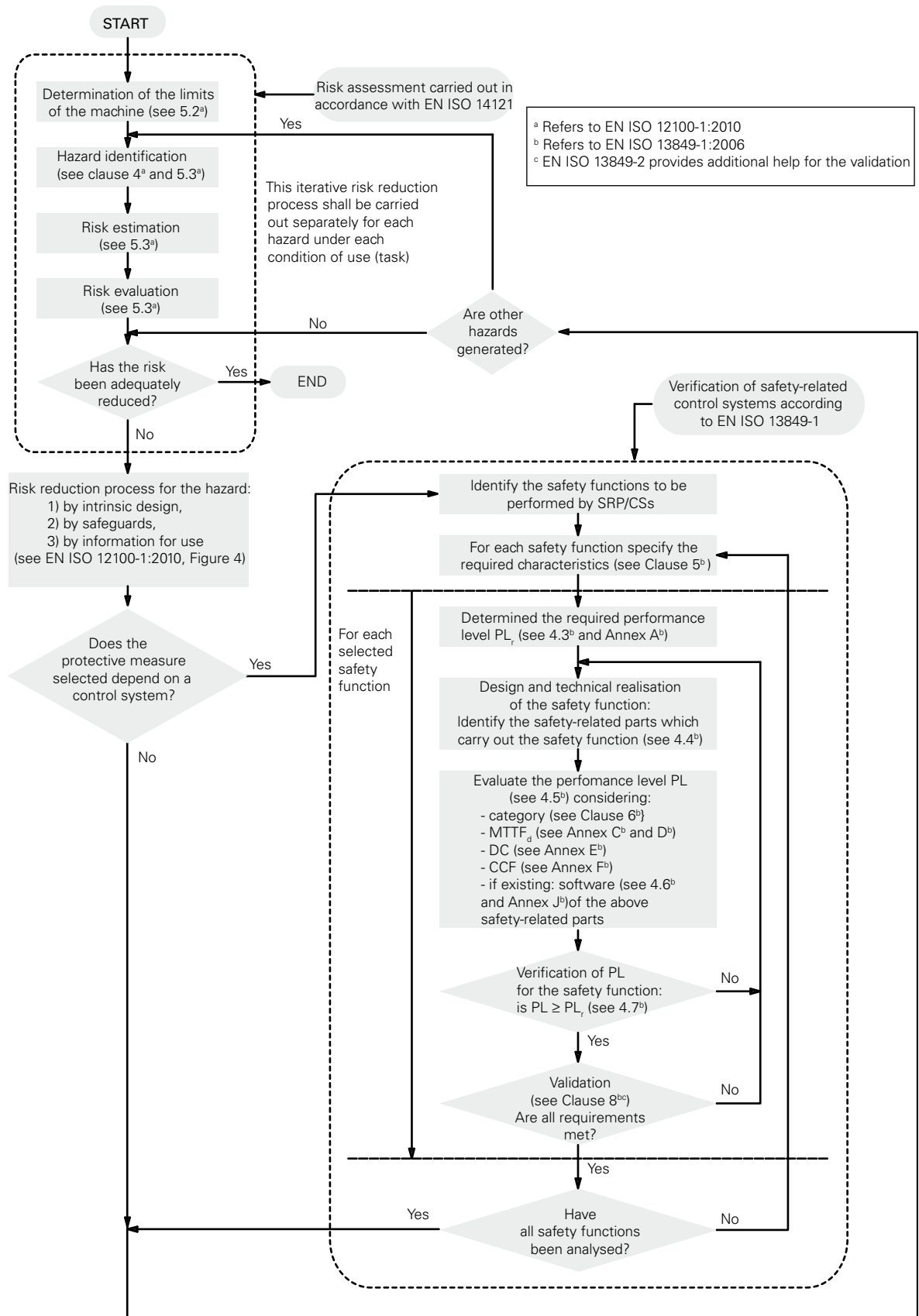
The methodology of risks analysis, their assessment, the procedure to their reduction is defined by EN ISO 12100 and EN ISO 14121 standards. These standards introduce an analysis cyclic model so that, fixed the initial targets, the risks analysis and possible solutions to reduce these risks are repeatedly evaluated till the targets are satisfied.

The model introduced by these standards provides for proceeding with the risks reduction/elimination after an analysis according to EN ISO 14121 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 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 13849-1:2006.

4 - Normative present situation (year 2011). 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.

Important note.

EN 13849 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.

In the functional safety field for control circuits safety, there are presently three standards in force (year 2011):

- EN 954-1:1996. It's a type B1 standard, which has introduced the Safety Categories concept, now near to expiration. The present EN 954-1:1996 will be in force up to December 2011, when it will be officially substituted by EN ISO 13849. However, since its great spread throughout the years, it will last for long as a technical reference.
- EN ISO 13849:2006. Type B1 standard which uses the PL concept.
- EN 62061:2005. Type B1 standard which uses the SIL concept.

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

The two standards EN 62061 and EN 13849 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 13849 table 1 and, as you can see, both standards can be applied for wide products typologies.

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

Technology implementing the safety-related control function	EN ISO 13849-1	IEC 62061
A Non electrical, e.g. hydraulics	X	Not covered
B Electromechanics, e.g. relays, or non complex electronics	Restricted to designated architectures ^a and up to PL=e	All architectures and up to SIL 3
C Complex electronics, e.g. programmable	Restricted to designated architectures ^a and up to PL=d	All architectures and up to SIL 3
D A combined with B	Restricted to designated architectures ^a and up to PL=e	X ^c
E C combined with B	Restricted to designated architectures ^a (see Note 1) and up to PL=d	All architectures and up to SIL 3
F C combined with A or C combined with A and B	X ^b	X ^c

X indicates that this item is dealt with by the International Standard shown in the column heading.

a. Designated architectures are defined in 6.2 (EN 13849-1) in order to give a simplified approach for quantification of performance level.

b. For complex electronics: use designated architectures according to this part of ISO 13849-1 up to PL = d or any architecture according to IEC 62061.

c. For non-electrical technology, use parts in accordance with this part of ISO 13849-1 as subsystems.

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 13849 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 13849 application where it is stated that the recommendations and restrictions for 13849 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.

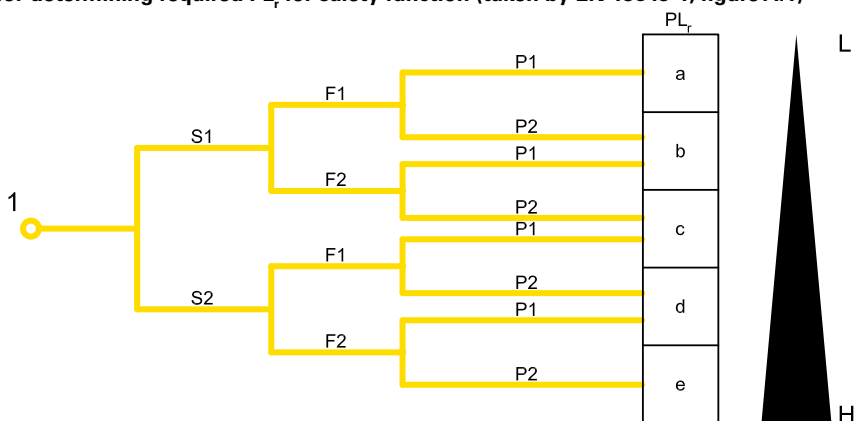
5 - EN ISO 13849 and new parameters: PL, MTTF_d, DC, CCF

EN ISO 13849 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. 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 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.

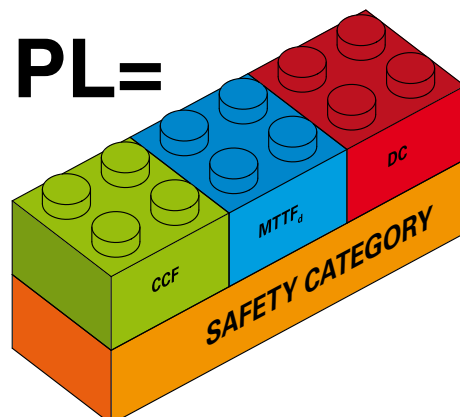
Required Category to EN 954-1:1996	Required Performance Level PL _r and required Category to EN ISO 13849-1:2006
B	→ b
1	→ c
2	→ d, Category 2
3	→ d, Category 3
4	→ e, Category 4

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 1×10^{-6} and 1×10^{-7} , that is about 1 dangerous failure every 100-1000 years.

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

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.





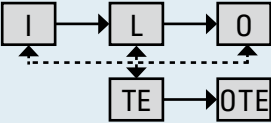
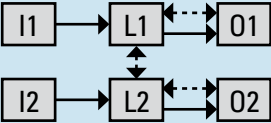
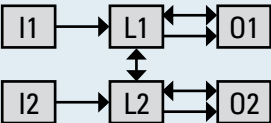
Safety Categories.

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 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	Principle 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 to Medium	None	Not relevant
1	Requirements of 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 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 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 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, but that if this detection is not possible, an accumulation of undetected faults shall 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.

Description	Range
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	60% < DC _{avg}

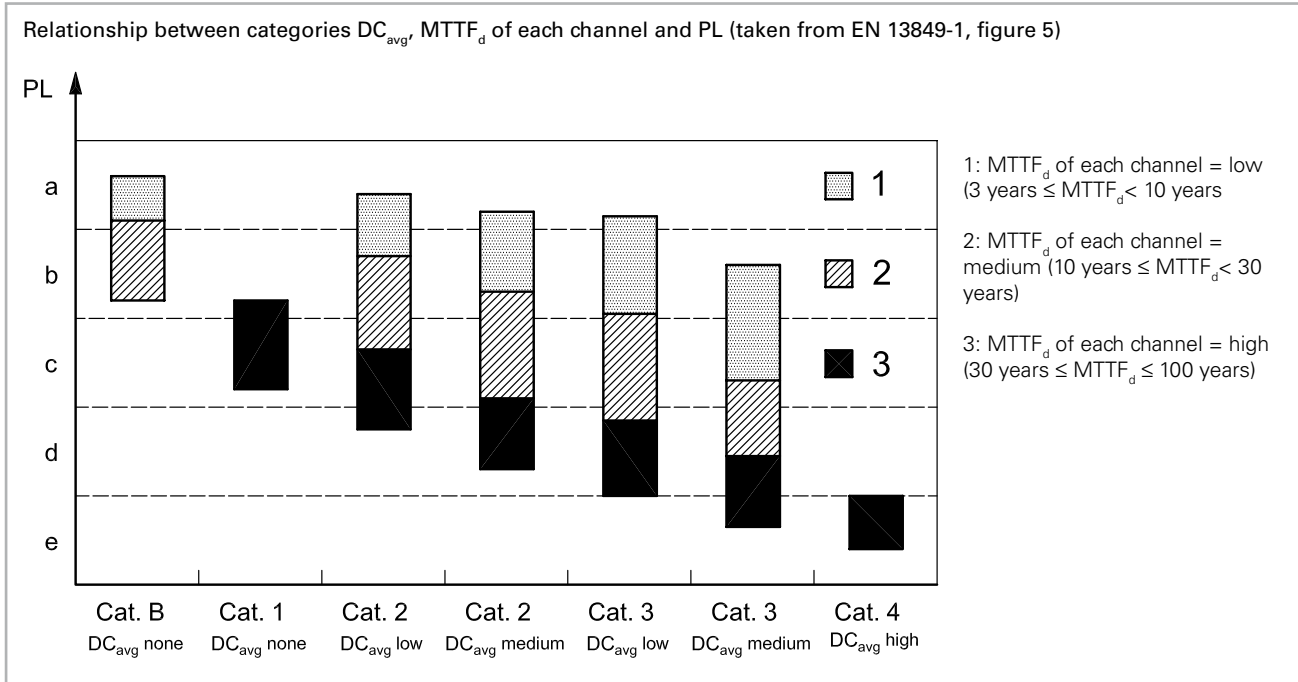
The None diagnostic coverage is admitted only for systems with architecture B or 1.

CCF ("Common Cause Failure")

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")

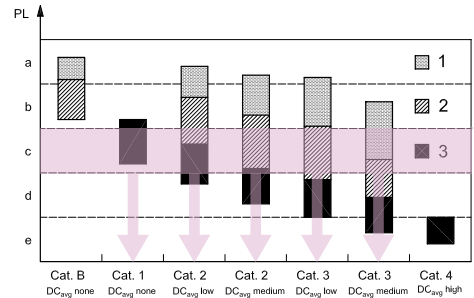
Knowing all this data, EN ISO 13849-1 determines the system PL by a correlation table (EN ISO 13849-1 Annex K) or by a simplified graphic figure (EN ISO 13849-1 paragraph 4.5) as follows.



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.

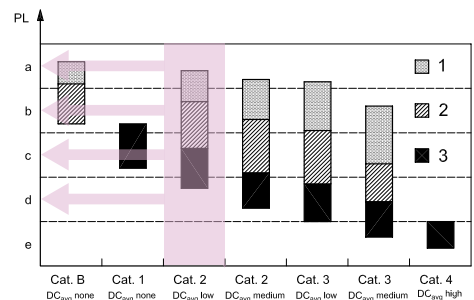
For instance, observing the figure, to obtain a system having a PL equal to "c" level all the following solutions are correct:

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 (2011)

The B10 and B10d data shown in the table refer to the mechanical life of the device safe contacts (NC with positive opening) in normal environmental condition. Mission time (for all items below mentioned): 20 years.

Series	Article description	B10	B10 _d	B10/ B10 _d
F•••••	Position switches	20.000.000	40.000.000	50%
F•••93 F•••92 F•••99 F•••R2	Safety switches with separate actuator	1.000.000	2.000.000	50%
FS, FG	Safety switches with solenoid and separate actuator	1.000.000	5.000.000	20%
F•••96 F•••95	Safety switches for hinged doors	1.000.000	5.000.000	20%
F•••C•	Safety switches with slotted hole lever	1.000.000	2.000.000	50%
F•••••	Rope safety switches with reset for emergency stop	1.000.000	2.000.000	50%
HP	Safety hinge switches	1.000.000	5.000.000	20%
SR	Coded magnetic sensor (connected with Pizzato safety modules)	10.000.000	20.000.000	50%
SR	Coded magnetic sensor (used with max load: 24V 250mA)	5.000.000	10.000.000	50%
PX, PA	Foot switches	20.000.000	40.000.000	50%
MK	Microswitches	10.000.000	20.000.000	50%
NA, NB, NF	Modular prewired switches	20.000.000	40.000.000	50%
E21PE•••••	Emergency pushbuttons	300.000	600.000	50%
E2C•••••	Contact blocks	20.000.000	40.000.000	50%

Code	Article description	MTTF _d	DC	PFH _d	SIL CL	PL	Cat
CS AM-01	Standstill monitor safety module	145	M	1.94E-09	2	d	3
CS AR-01	Safety module for guards monitoring and emergency stop	147	H	6.38E-10	3	e	4
CS AR-02	Safety module for guards monitoring and emergency stop	147	H	6.38E-10	3	e	4
CS AR-04	Safety module for guards monitoring and emergency stop	147	H	6.38E-10	3	e	4
CSAR-04V024	Safety module for guards monitoring and emergency stop	218	H	4.58E-10	3	e	4
CS AR-05	Safety module for guards monitoring, emergency stop, light curtains	147	H	6.61E-10	3	e	4
CSAR-05V024	Safety module for guards monitoring, emergency stop, light curtains	218	H	4.58E-10	3	e	4
CS AR-06	Safety module for guards monitoring, emergency stop, light curtains	147	H	6.61E-10	3	e	4
CSAR-06V024	Safety module for guards monitoring, emergency stop, light curtains	218	H	4.58E-10	3	e	4
CS AR-07	Safety module for guards monitoring and emergency stop	111	H	7.56E-10	3	e	4
CS AR-08	Safety module for guards monitoring, emergency stop, light curtains	218	H	4.58E-10	3	e	4
CS AR-20	Safety module for guards monitoring and emergency stop	358	M	8.71E-09	3	e	3
CS AR-21	Safety module for guards monitoring and emergency stop	358	M	8.71E-09	3	e	3
CS AR-22	Safety module for guards monitoring and emergency stop	201	H	8.87E-09	3	e	3
CS AR-23	Safety module for guards monitoring and emergency stop	201	H	8.87E-09	3	e	3
CS AR-24	Safety module for guards monitoring and emergency stop	111	H	1.18E-09	3	e	3
CS AR-25	Safety module for guards monitoring and emergency stop	111	H	1.18E-09	3	e	3
CS AR-40	Safety module for guards monitoring and emergency stop	356	M	1.08E-08	2	d	2
CS AR-41	Safety module for guards monitoring and emergency stop	356	M	1.08E-08	2	d	2
CS AR-46	Safety module for guards monitoring and emergency stop	435	-	3.32E-08	1	c	1
CS AR-51	Safety module for safety mats and safety edges monitoring	209	H	9.43E-09	3	e	4
CS AR-90	Safety module for lift automatic floor levelling	382	H	5.03E-10	3	e	4
CS AR-94	Safety module for lift automatic floor levelling	213	H	5.62E-09	3	e	4
CS AR-95	Safety module for lift automatic floor levelling	213	H	5.42E-09	3	e	4
CS AT-0x	Safety timed module for guards monitoring and emergency stop	84	H	9.01E-09	3	e	4
CS AT-1x	Safety timed module for guards monitoring and emergency stop	84	H	9.01E-09	3	e	4
CS AT-3x	Safety timed module for guards monitoring and emergency stop	74	H	4.05E-09	3	e	4
CS DM-01	Safety module for bimanual control	142	H	2.99E-08	3	e	4
CS DM-02	Safety module for bimanual control	206	H	2.98E-08	3	e	4
CS FS-10	Safety timer module	146	H	1.62E-09	3	e	4
CS FS-20	Safety timer module	205	M	1.10E-08	2	d	3
CS FS-30	Safety timer module	205	M	1.10E-08	2	d	3
CS FS-50	Safety timer module	349	M	1.17E-08	2	d	3
CS ME-01	Contacts expansion module	76	H	6.38E-10	3	e	4
CS ME-02	Contacts expansion module	113	H	2.84E-09	3	e	4
CS ME-03	Contacts expansion module	208	M	2.45 E-08	2	d	3
CS ME-20	Contacts expansion module	113	H	3.07E-09	3	e	4
CS ME-30	Contacts expansion module	112	H	2.77E-09	3	e	4
CS ME-31	Contacts expansion module	112	H	2.77E-09	3	e	4

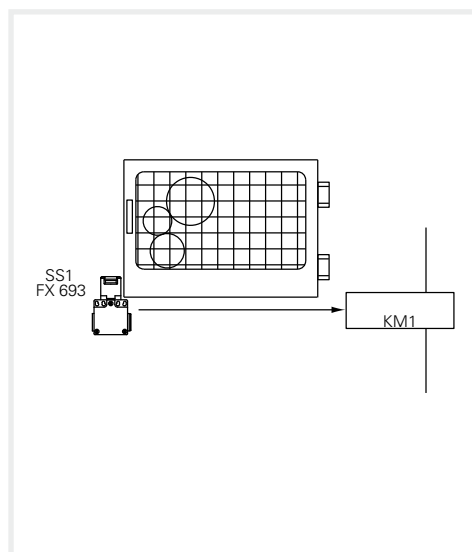
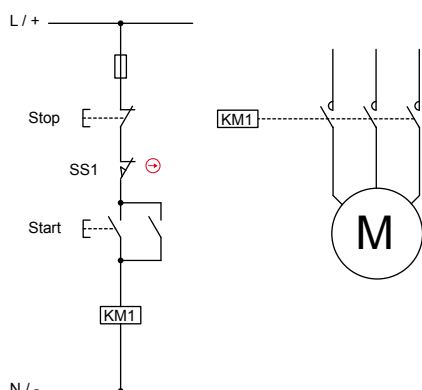
B10_d: Number of operations until 10% of components fail dangerously
 B10: Number of operations until 10% of components fail
 B10/B10_d: dangerous failures and total failures ratio
 MTTF_d: Mean Time To Failure Dangerous

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

EXAMPLE 1 Application: Guards control

Reference standard EN ISO 13849-1:2006

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 .

Safety function description

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 push 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.

Devices data:

- SS1 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 $B10_d$ value is supplied by the manufacturer (see page 7/32) 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 and its $B10_d$ value is equal to 2,000,000 operations. This value is determined from the standard tables (see EN ISO 13849-1 table C.1).

Working frequency hypothesis

- 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 $N_{op} = (365 \times 24 \times 3,600) / 600 = 52,560$.
- Assuming the start button operation every 300 seconds, 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: $MTTF_d = B10_d / (0,1 \times N_{op}) = 2,000,000 / (0,1 \times 52,560) = 381$ years
- The $MTTF_d$ of the KM1 contactor is equal to: $MTTF_d = B10_d / (0,1 \times N_{op}) = 2,000,000 / (0,1 \times 157,680) = 127$ years
- In consequence the one channel circuit $MTTF_d$ is equal to: $1 / (1/381 + 1/127) = 95$ years.

DC_{avg} Diagnostic Coverage

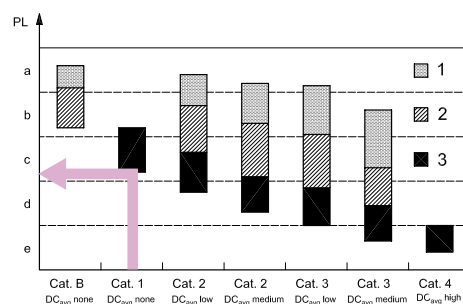
No measures for fault detection are implemented therefore the diagnostic coverage is None, admitted condition for the considered circuit which is in category 1.

CCF Common Cause Failure

No CCF calculation is necessary for a category 1 circuit.

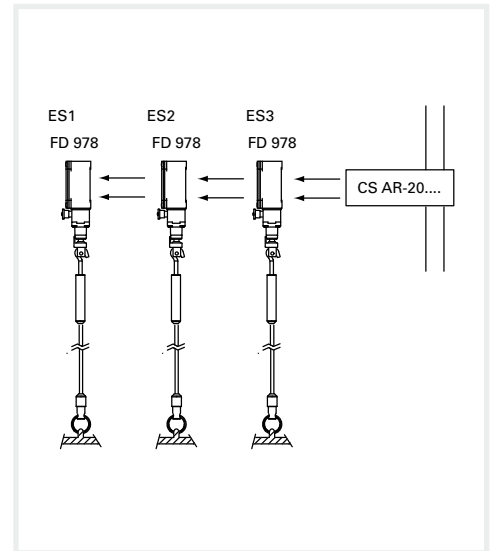
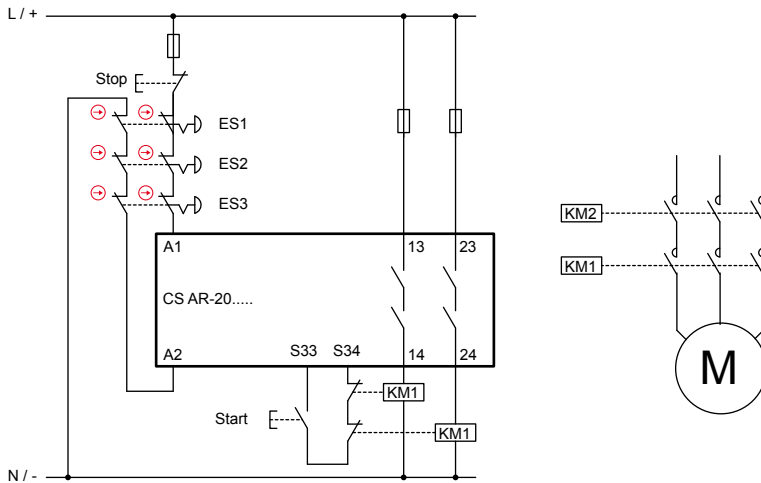
PL verification

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 13849-1:2006	
Safety category	3
Performance Level	PL e



Safety function description

The operation of one emergency device causes the safety module and the two contactors KM1 and KM2 to intervene. The ES1, ES2, ES3 devices signal is redundantly monitored by the CS safety module. KM1 and KM2 contactors (with forcedly guided contacts) are also monitored by CS safety module through the circuit feedback.

Devices data:

- ES1, ES2, ES3 (FD 978) are rope switches for emergency stop with positive opening. The device B_{10_d} value is equal to 2,000,000 (see page 7/32)
- KM1, KM2 are contactors used at nominal value. The device B_{10_d} value is equal to 2,000,000 (see EN ISO 13849-1 Table C.1)
- CS is a safety module (CS AR-20) with $MTTF_d=358$ years (see page 7/32) and DC= Medium
- The circuit architecture is two channels type in category 3

Working frequency hypothesis

- 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
- $MTTF_d CS = 358$ years
- $MTTF_d CH1 = 349$ years. Value restricted to 100 years. The channels are symmetric thus $MTTF_d=100$ years (High)

DC_{avg} Diagnostic Coverage

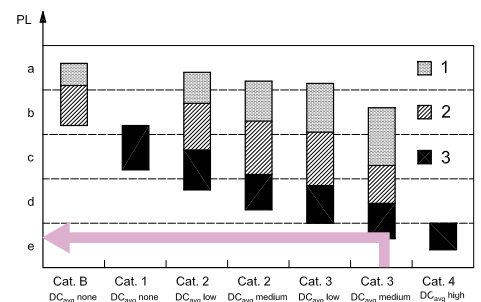
- KM1 and KM2 contactors are monitored by CS through the circuit feedback. DC=99% (High)
- The CS AR-20 safety module has a Medium diagnostic coverage.
- Not all faults in the emergency devices series can be detected. The diagnostic coverage is 90% (Medium)

CCF Common Cause Failure

It is assumed a score > 65 (according to 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.

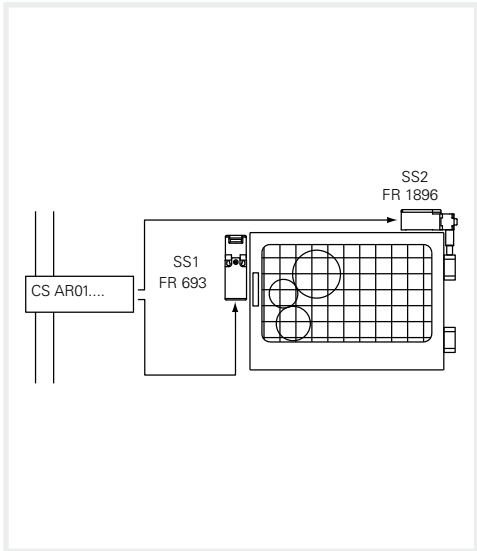
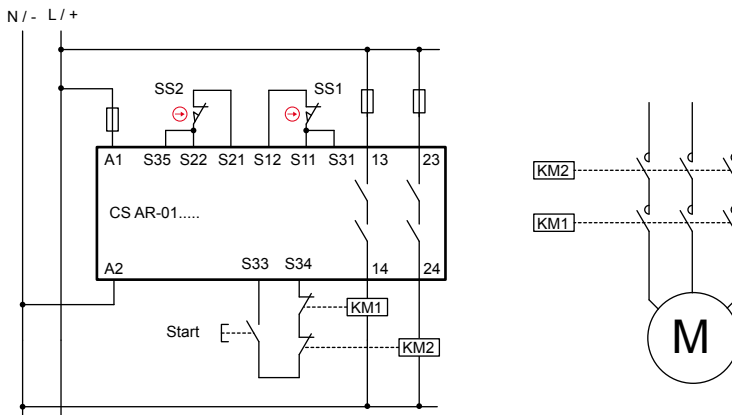


EXAMPLE 3

Application: Guards control

Reference standard EN ISO 13849-1:2006

Safety category **4**
Performance Level **PL e**



Safety function description

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 devices signal is redundantly monitored by the CS safety module.

The switches have a different working principle.

KM1 and KM2 contactors (with forcibly guided contacts) are also monitored by CS safety module through the circuit feedback.

Devices data:

- SS1 (FR 693) is a switch with positive opening. The $B10_d$ is equal to 2,000,000 (see page 7/32)
- SS2 (FR 1896) is a hinge operating switch with positive opening. $B10_d = 5,000,000$ (see page 7/32)
- KM1, KM2 are contactors used at nominal value. $B10_d = 2,000,000$ (see EN ISO 13849-1 Table C.1)
- CS is a safety module (CS AR-01) with $MTTF_d = 147$ years and $DC = 99\%$ (High)

Working frequency hypothesis

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

MTTF_d Calculation

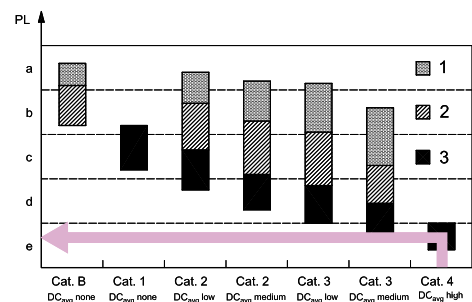
- $MTTF_{d, SS1} = 228$ years
- $MTTF_{d, SS2} = 571$ years
- $MTTF_{d, KM1, KM2} = 228$ years
- $MTTF_{d, CS} = 147$ years
- $MTTF_{d, CH1} = 64$ years (SS1, CS, KM1)
- $MTTF_{d, CH2} = 77$ years (SS2, CS, KM2)
- $MTTF_{d, symmetrical} = 70,5$ years (High)

DC_{avg} Diagnostic Coverage

- SS1, SS2 have $DC = 99\%$ since SS1, SS2 contacts are monitored by the CS and they have different working principles.
- KM1 and KM2 contacts are monitored by CS through the circuit feedback. $DC = 99\%$ (High)
- The CS inside has a redundant and self-monitoring circuit. $DC = 99\%$ (High)
- $DC_{avg} = 99\%$ (High)

PL verification

A category 4 circuit with $MTTF_d = 70,5$ years and $DC_{avg} = High$ corresponds to a PL e.



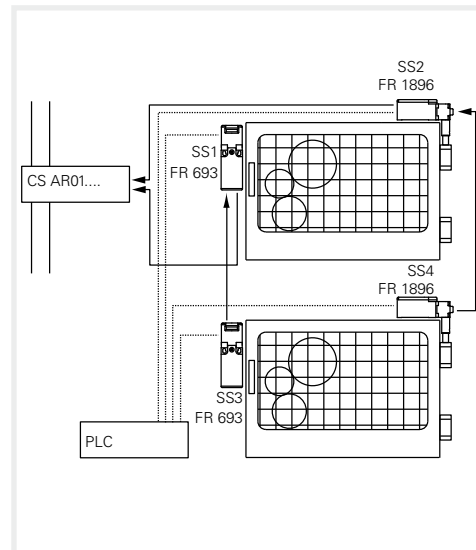
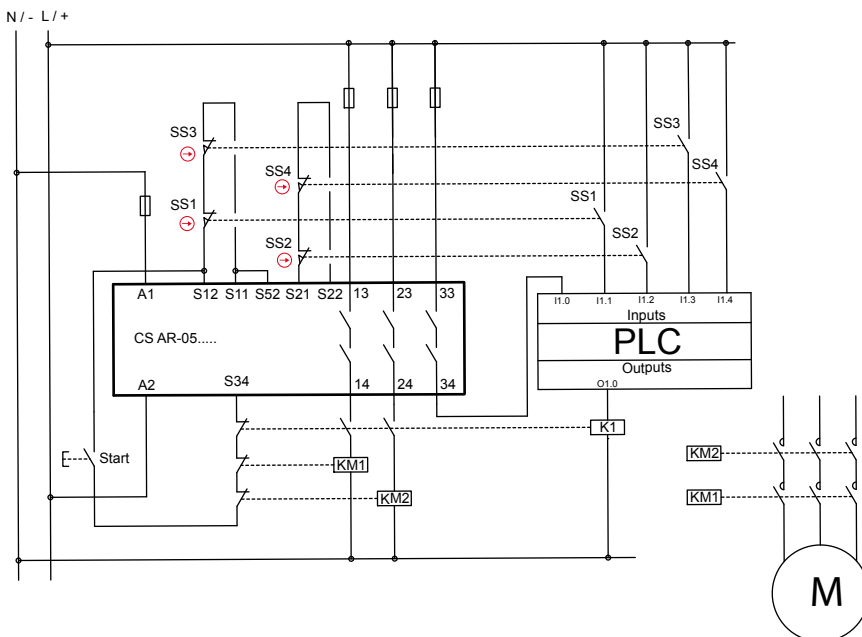
EXAMPLE 4**Application: Guards control**

Reference standard EN ISO 13849-1:2006

Safety category

4

Performance Level

PL e**Safety function description**

A guard opening causes the SS1, SS2 switches to intervene on the first guard and SS3, SS4 on the second; the switches make the safety module and the KM1 and KM2 contactors intervene.

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

The switches have a different working principle.

KM1 and KM2 contactors (with forcibly guided contacts) are also monitored by CS safety module through the circuit feedback.

Devices data:

- SS1, SS3 (FR 693) are switches with positive opening. The $B10_d$ is equal to 2,000,000 (see page 7/32)
- SS2, SS4 (FR 1896) is a hinge operating switch with positive opening. $B10_d = 5,000,000$ (see page 7/32)
- KM1, KM2 are contactors used at nominal value. The $B10_d$ is equal to 2,000,000 (see EN ISO 13849-1 Table C.1)
- CS is a safety module (CS AR-05) with $MTTF_d = 147$ years and $DC = 99\%$

Working frequency hypothesis

- 4 times per hour for 24 h/day and 365 days/year equal to $n_{op}/year = 35,040$
- Contactors shall intervene 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
- $MTTF_{d, CS} = 147$ years
- $MTTF_{d, Ch1} = 72$ years (SS1, SS3, CS, KM1)
- $MTTF_{d, Ch2} = 85$ years (SS2, SS4, CS, KM2)
- $MTTF_d$: symmetrically arranging the 2 channels, the result is $MTTF_d = 79$ years (High)

DC_{avg} Diagnostic Coverage

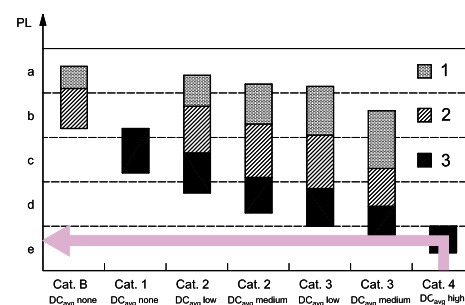
- KM1 contacts are monitored by CS through the circuit feedback. $DC = 99\%$
- All the switches auxiliary contacts are monitored by PLC. $DC = 99\%$
- The module CS AR-05 have a $DC = 99\%$ (see page 7/32)
- The diagnostic coverage for both channels is 99% (High)

CCF Common Cause Failure

- It is assumed a score > 65 (according to EN ISO 13849-1 annex F).

PL verification

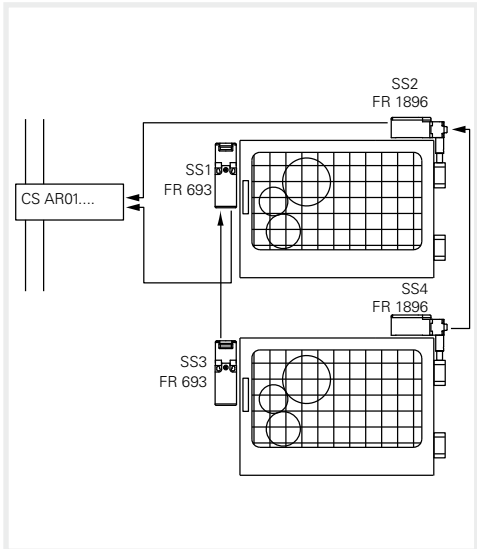
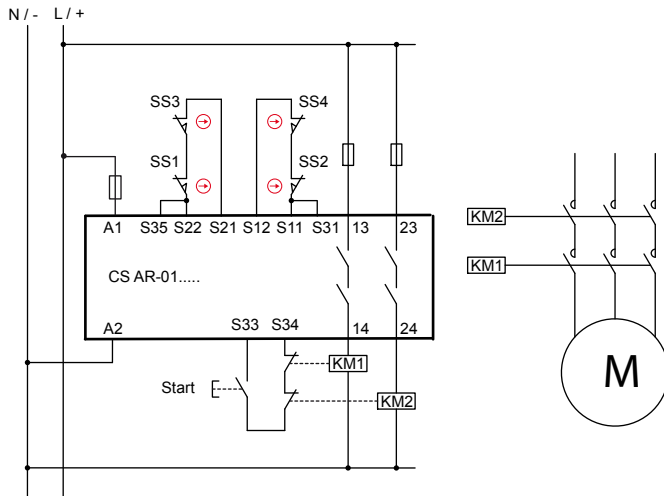
- A category 4 circuit with $MTTF_d = 79$ years (High) and $DC_{avg} = \text{High}$ corresponds to a PL e.



EXAMPLE 5 Application: Guards control

Reference standard EN ISO 13849-1:2006

Safety category **3**
Performance Level **PL e**



Safety function description

A guard opening causes the SS1, SS2 switches to intervene on the first guard and SS3, SS4 on the second; the switches make the safety module and the KM1 and KM2 contactors intervene.

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

The switches have a different working principle.

KM1 and KM2 contactors (with forcibly guided contacts) are also monitored by CS safety module through the circuit feedback.

Devices data:

- SS1, SS3 (FR 693) are switches with positive opening. The B_{10_d} is equal to 2.000.000 (see page 7/32)
- SS2, SS4 (FR 1896) is a hinge operating switch with positive opening. B_{10_d} = 5.000.000 (see page 7/32)
- KM1, KM2 are contactors used at nominal value. The B_{10_d} is equal to 2.000.000 (see EN ISO 13849-1 Table C.1)
- CS is a safety module (CS AR-01) with $MTTF_d$ = 147 years and DC = 99%

Working frequency hypothesis

- Twice per hour for 16 h/day and 365 days/year equal to $n_{op}/year$ = 11.680
- Contactors shall intervene 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
- $MTTF_{d, CS}$ = 147 years
- $MTTF_{d, CH1}$ = 109 years (SS1, SS3, CS, KM1)
- $MTTF_{d, CH2}$ = 118 years (SS2, SS4, CS, KM2)
- $MTTF_{d}$ = value restricted to 100 years

DC_{avg} Diagnostic Coverage

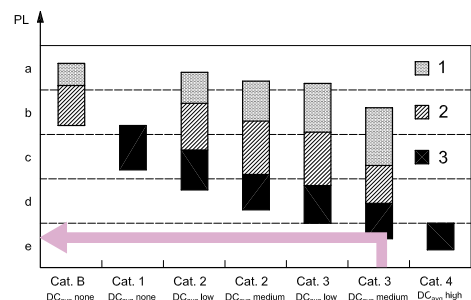
- KM1 contacts are monitored by CS through the circuit feedback. DC = 99%
- Not all faults in the switches series can be detected. DC = 60%
- The CS AR-01 module has a DC = 99%
- It is assumed a diagnostic coverage is 92% (Medium)

CCF Common Cause Failure

- It is assumed a score > 65 (according to EN ISO 13849-1 annex F).

PL verification

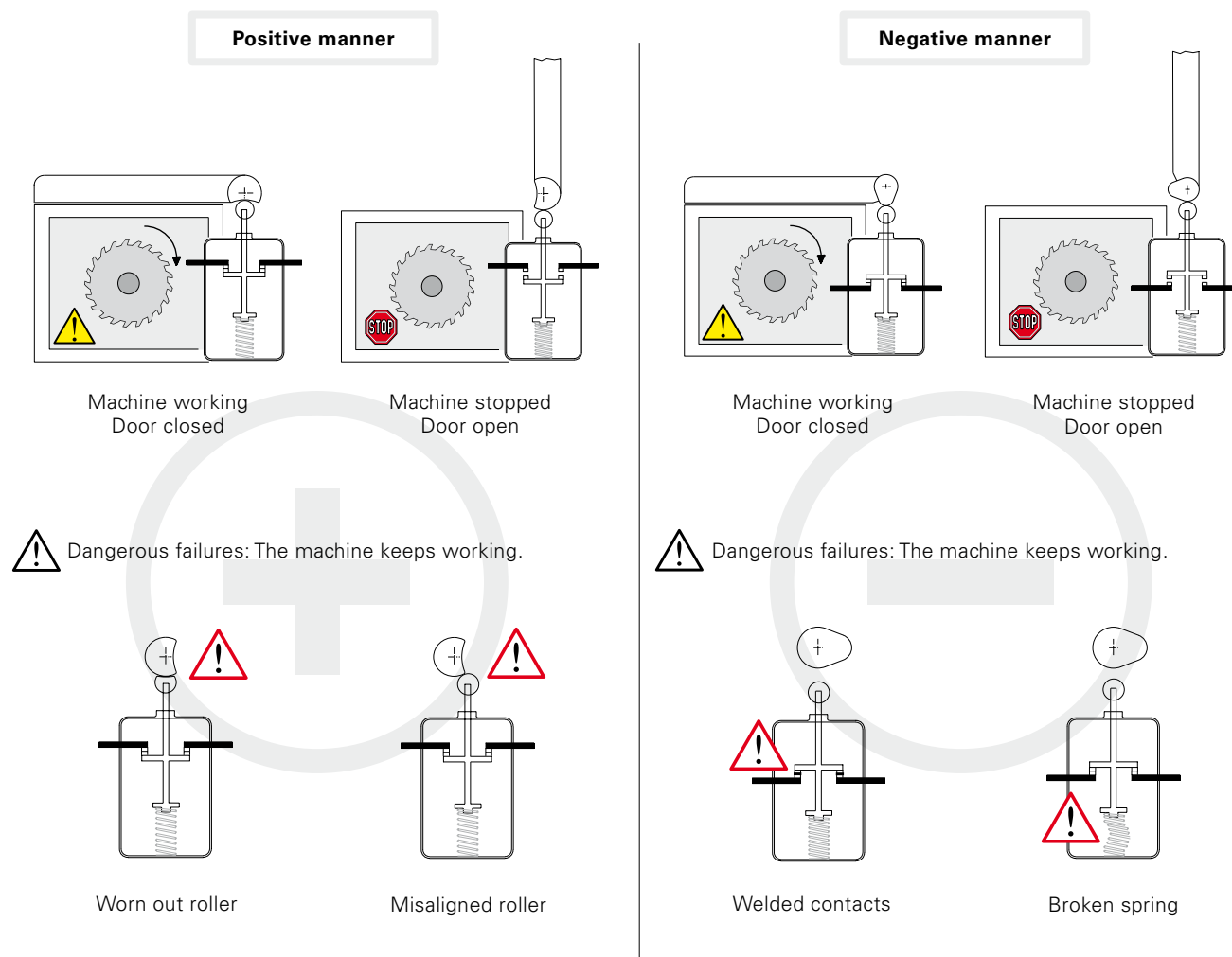
- A category 3 circuit with $MTTF_{d}$ = 100 years and DC_{avg} = medium corresponds to a PL e.



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

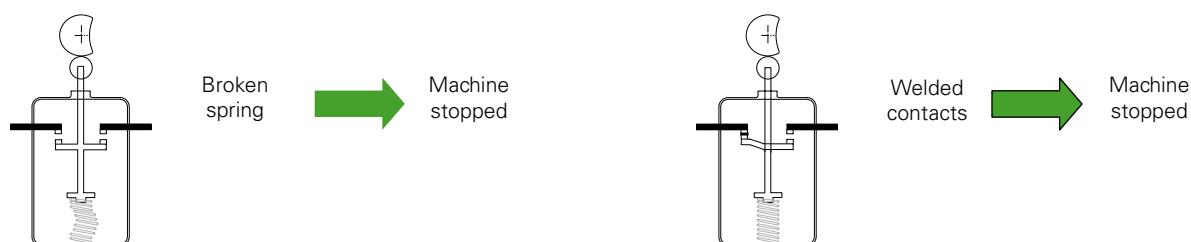
Positive manner and negative manner.

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**.




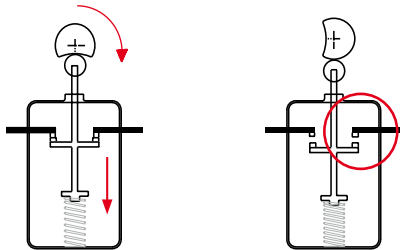
The positive manner avoids, with a preventive maintenance, the dangerous failures indicated above. On the contrary, the negative manner failures occur inside the switch and are therefore difficult to be detected.

With the positive manner, 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 manners, for example:

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

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

Diversification

Safety in the redundant system is increased by **diversification**. It is obtained by the application of two limit switches with different project 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 and one hinge operated FR 1896 switch).

Redundancy

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

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.