

How to choose between EN/ISO 13849 and EN/IEC 62061

Select the applicable standard

Based on the generic definition of the risk, the standards classify necessary safety levels in different discrete levels corresponding for each one to a probability of dangerous failure per hour:

- > PL (Performance Level) for standard EN/ISO 13849-1
- > SIL (Safety Integrity Level) for standard EN/IEC 62061

The table below gives the relationship between the performance level (PL) and the Safety Integrity Level (SIL).

PL	ISL	Probability of dangerous failures per hour 1/h
a	No correspondance	$\geq 10^{-5} \dots < 10^{-4}$
b	1	$\geq 3 \times 10^{-6} \dots < 10^{-5}$
c	1	$\geq 10^{-6} \dots < 3 \times 10^{-6}$
d	2	$\geq 10^{-7} \dots < 10^{-6}$
e	3	$\geq 10^{-8} \dots < 10^{-7}$

Recommended application of IEC 62061 and ISO 13849-1

Annex	Technology implementing the safety related control function (S)	ISO 13849-1	IEC 62061
A	Non electrical, e.g. hydraulics	X	Not covered
B	Electromechanical, e.g. relays, or non-complex electronics	Restricted to designated architectures (see Note 1) and up to PL=e	All architectures and up to SIL 3
C	Complex electronics, e.g. programmable	Restricted to designated architectures (see Note 1) and up to PL=d	All architectures and up to SIL 3
D	A combined with B	Restricted to designated architectures (see Note 1) and up to PL=e	X see Note 3
E	C combined with B	Restricted to designated architectures (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 see Note 2	X see Note 3

"X" indicates that this item is dealt with by the standard shown in the column heading.

Note 1 Designated architecture are defined in Annex B of EN/ISO 13849-1 to give a simplified approach for qualification of performance level

Note 2 For complex electronics: use of designated architecture according to EN/ISO 13849-1 up to PL=d or any architecture according to EN/IEC 62061

Note 3 For non-electrical technology use parts according to EN/ISO 13849-1 as subsystems.

For building specific complex sub-systems or for higher level requirements including software, standard EN/IEC 61508 relating to systems must be used.

Standard EN/ISO 13849-1
Standards to be applied according to the design selected for the safety-related machine control system

Introduction to Functional Safety of Machinery

The functional safety standards are intended to encourage designers to focus more on the functions that are necessary to reduce each individual risk, and on the performance required for each function, rather than simply relying on particular components. These standards make it possible to achieve greater levels of safety throughout the machine's life.

- > Under the previous standard, EN 954-1, categories (B, 1, 2, 3 and 4) dictated how a safety-related electrical control circuit must behave under fault conditions. Designers can follow either EN/ISO 13849-1 or EN/IEC 62061 to demonstrate conformity with the Machinery Directive. These two standards consider not only whether a fault will occur, but also how likely it is to occur
- > This means there is a quantifiable, probabilistic element in compliance: machine builders must be able to determine whether their safety circuit meets the required safety integrity level (SIL) or performance level (PL). Panel builders and designers should be aware that manufacturers of the components used in safety circuits (such as safety detection components, safety logic solvers and output devices like contactors) must provide detailed data on their products

Standard EN/ISO 13849-1 Machinery safety - Safety-related parts of control systems

Standard EN/ISO 13849-1 is an evolution of standard EN 954-1.

Field of application of the standard

This standard gives safety requirements and advice relating to principles for the design and integration of safety-related parts of control systems (SRP/CS), including software design. For these parts, it specifies the characteristics, including the performance level, needed to achieve these safety functions. It applies to the SRP/CS of all types of machine, regardless of the technology and type of energy used (electric, hydraulic, pneumatic, mechanical, etc.).

Process

Risk assessment as defined in standard EN/ISO 12100 leads to decisions on risk reduction measures.

If these measures depend on a control system, then EN/ISO 12100 can apply. It defines a **6-stage design process**:

- 1 - Selection of the essential safety functions that SRP/CS must perform. For each safety function, specify the required characteristics
- 2 - Determine the required performance level (PLr)
- 3 - Design and technical creation of safety functions: identify the parts that perform the safety function
- 4 - Evaluate the performance level PL for each safety-related part
- 5 - Check that the performance level PL achieved is greater than or equal to the required level (PLr)
- 6 - Check that all requirements are satisfied

We will now illustrate these stages, taking as an example a safety function where a severe injury can be caused by a trolley not stopping at the end of the Jib and thus causing the trolley to fall. A person can be exposed to this dangerous situation around the hoisting machine.

Stage 1 - Selection of safety functions

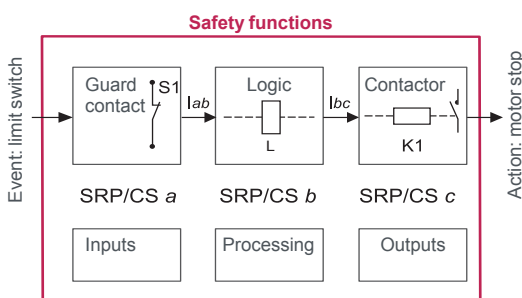
The diagram opposite shows a safety function which consists of several parts:

- > The input actuated by opening of the guard (SRP/CSa)
- > The control logic, limited in this example to opening or closing of a contactor coil (SRP/CSb)
- > The power output that controls the motor (SRP/CSc)
- > The connections (lab, lbc)

Stage 2 - Estimation of required performance level (PLr)

Considering our example of the person coming into area where the dangerous hoisting machine is operating we now estimate the risk using the risk graph. The parameters to be considered are:

- > **S** Severity of the injury
 - > **S1** Slight injury, normally reversible
 - > **S2** Serious, normally irreversible, including death
- > **F** Frequency and/or duration of exposure to the hazardous phenomenon
 - > **F1** Rare to fairly frequent and/or short duration of exposure
 - > **F2** Frequent to permanent and/or long duration of exposure
- > **P** Possibility of avoiding the hazardous phenomena or limiting the harm
 - > **P1** Possible under certain circumstances
 - > **P2** Virtually impossible



Representation of the safety function

Risk related to the potential hazard

=

Severity of the potential harm

X

Probability of occurrence:
- Frequency and duration of exposure
- Possibility of avoiding or limiting the probability of the occurrence of an event that could cause the harm

Standard EN/ISO 13849-1

Machinery safety - Safety-related parts of control systems (continued)

Process (continued)

Stage 2 - Estimation of required performance level (PLr) (continued)

For our example: a serious injury S1 can be caused by being exposed near the hoisting machine as if there is no safe guarding to ensure the trolley stops the load and trolley will fall. After considering the severity of the injury we investigate the frequency and/or duration of the possible entry to the dangerous area. Here we define the frequency of exposure to the hazard is low F1 (occasional presence) as there are restrictions to enter the area. The last step is based upon the possibility to avoid the hazard and limiting the harm. To evaluate this we take into consideration that it is possible to avoid the harm as the visibility around the dangerous machine is monitored by the operator and in this case there is a possibility to avoid the harm under certain conditions so we define it as P1.

The result of the estimation gives a required performance level PLr = c.

Stage 3 - Design and creation of the safety functions

At this point, we need to describe the PL calculation method.

For a SRP/CS (or a combination of SRP/CS), PL could be estimated with the figure shown on page 1/19, after estimation of several factors such as :

- > Hardware and software system structure (categories)
- > Mechanism of failures, diagnostic coverage (DC)
- > Components reliability, Mean Time To dangerous Failure (MTTF_d)
- > Common Cause Failure (CCF)

> Categories (Cat.) and designated architectures

The table below summarises system behaviour in the event of a failure and the principles used to achieve the safety, for the 5 categories defined:

Cat.	System behaviour	Designated architectures
B	A fault can lead to loss of the safety function	
1	As for category B but the probability of this occurrence is lower than for the category B	
2	A fault can lead to loss of the safety function between two periodic inspections and loss of the safety function is detected by the control system at the next test.	
3	For a single fault, the safety function is always ensured. Only some faults will be detected. The accumulation of undetected faults can lead to loss of the safety function.	
4	When faults occur, the safety function is always ensured. Faults will be detected in time to prevent loss of the safety function	

Key:

im: Interconnecting means

c: Cross monitoring

I, I1, I2: Input device, e.g. sensor

L, L1, L2: Logic

m: Monitoring

O, O1, O2: Output device, e.g. main contactor

TE: Test equipment

OTE: Output of TE

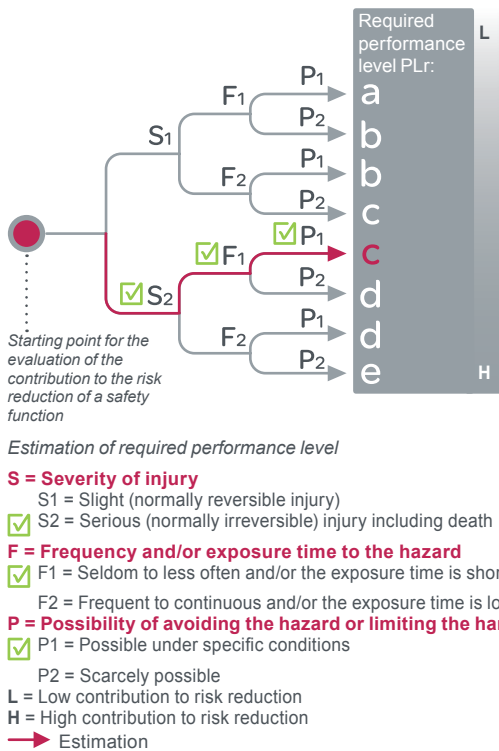
> MTTF_d (Mean Time To dangerous Failure)

The value of the MTTF_d of each channel is given in 3 levels (see table below) and shall be taken into account for each channel (e.g. single channel, each channel of a redundant system) individually.

Reliability levels of components

Index	Range
Low	3 years ≤ MTTF _d < 10 years
Medium	10 years ≤ MTTF _d < 30 years
High	30 years ≤ MTTF _d < 100 years

A MTTF_d of less than 3 years should never be found, because this would mean that after one year in operation, 30% of all those components in use would have failed to a dangerous state. The maximum value is limited to 100 years because devices dealing with a significant risk should not depend on the reliability of a single component. Additional measures such as redundancy and tests are required.



Standard EN/ISO 13849-1
Standards to be applied according to the design selected for the safety-related machine control system

Standard EN/ISO 13849-1
Machinery safety - Safety-related parts of control systems (*continued*)
Process (*continued*)

Stage 3- (*continued*)

> Diagnostic coverage (DC): this term is expressed as a percentage and quantifies the ability to diagnose a dangerous failure

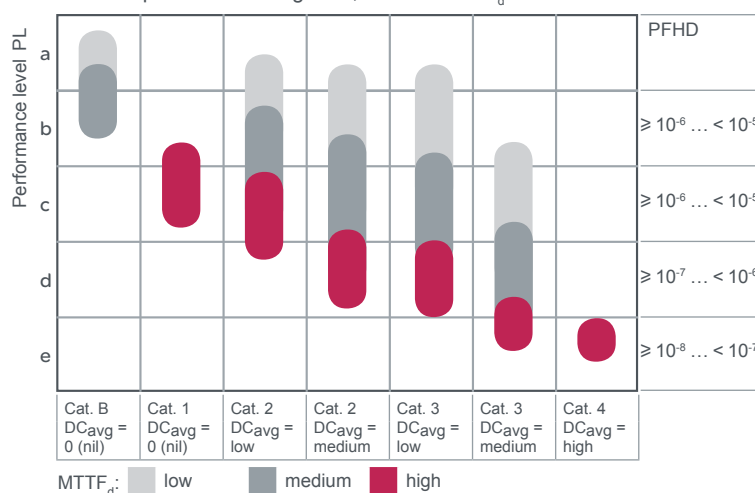
For example, in the event of welding of a N/C contact in a relay, the state of the N/O contact could incorrectly indicate the opening of the circuit, unless the relay has mechanically linked N/O and N/C contacts, when the fault can be detected.

The standard recognises four levels:

Diagnostic coverage (DC)

Denotation	Range
Nil	DC < 60%
Low	60% ≤ DC < 90%
Medium	90% ≤ DC < 99%
High	99% ≤ DC

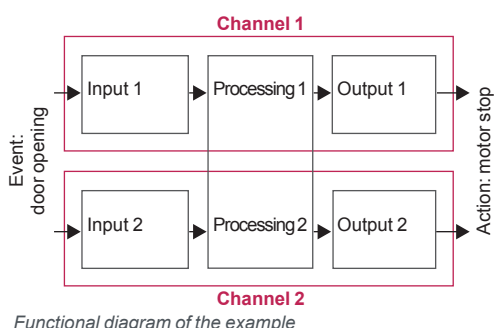
> Relationship between Categories, DC and MTTF_d of each channel and the PL



> Using the above chart we can now select the most appropriate architecture, the required Diagnostic coverage as well as ensure the products selected have the right MTTF_d values

> As we require PL= "c" the chart states as a minimum a category 1 architecture with a Diagnostic coverage of 0 (Nil) and a MTTF_d of High is required. It is possible to use architectures with higher categories to solve the safety function needs

> We start with determining the architecture required to solve the function. We use the following Category 1 architecture (see page 1/19)

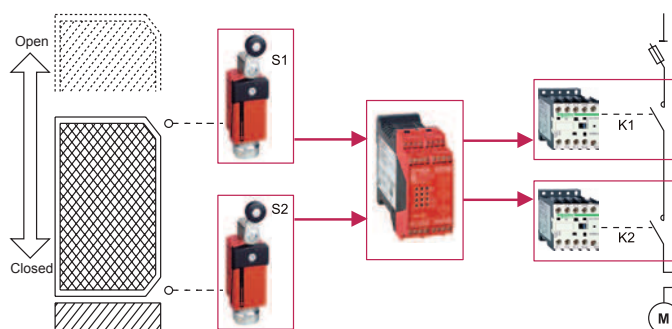


> In our example, to reach the PL = e, the solution will therefore have to correspond to category 4 with redundant circuit; the function scheme is shown opposite with two channels in parallel

> a high diagnostic capability

> a high MTTF_d

For our application, we could suggest a redundant relay scheme but it is nowadays easier to use safety function blocks. The solution is illustrated below.



The process suggested by the standard is iterative and a few estimations are therefore necessary in order to obtain the expected result. In view of the required performance level, we have chosen a solution with redundant circuit.

Standard EN/ISO 13849-1

Machinery safety - Safety-related parts of control systems (continued)

Process (continued)

Stage 4 - Evaluate the performance level PL for each safety-related part

Based on the information in the supplier's catalogue and Annex E of the standard, we obtain the following values:

Example	B ₁₀ (number of operations) / % dangerous failure	MTTF _d	DC
SRP/CS _a : Safety limit switches	10.000.000 / 20% dangerous failure	7102	99%
SRP/CS _b : XPS AK safety module	-	154.5	99.99%
SRP/CS _c : LCK contactor	1.000.000 / 73% dangerous failure	194	99%

For electromechanical products, the MTTF_d is calculated on the basis of the total number of operations that the product can perform, using B_{10d} values:
In our case, the machine operates for 220 days per year, 8 hours per day with a cycle of 90 s.

$$N = 220 \times 8 \times (3600 / 90) = 70\,400 \text{ operations/year}$$

$$\text{MTTF}_d = B_{10d} / (0.1 \times N) \text{ and } B_{10d} = B_{10} / \% \text{ dangerous failure.}$$

For the safety switches,

$$\text{the MTTF}_d = (1 / 0.20 \times 10\,000\,000) / (0.1) \times 70\,400 = 7102 \text{ years}$$

For the contactors,

$$\text{the MTTF}_d = (1 / 0.73 \times 1\,000\,000) / (0.1) \times 70\,400 = 194 \text{ years}$$

The MTTF_d for each channel will then be calculated using the formula:

$$\frac{1}{\text{MTTF}_d} = \frac{1}{\text{MTTF}_{da}} + \frac{1}{\text{MTTF}_{db}} + \frac{1}{\text{MTTF}_{dc}}$$

i.e. 85 years for each channel.

A similar formula is used to calculate the diagnostic capability

$$\text{DC}_{\text{avg}} = \frac{\frac{\text{DC}_a}{\text{MTTF}_{da}} + \frac{\text{DC}_b}{\text{MTTF}_{db}} + \frac{\text{DC}_c}{\text{MTTF}_{dc}}}{\frac{1}{\text{MTTF}_{da}} + \frac{1}{\text{MTTF}_{db}} + \frac{1}{\text{MTTF}_{dc}}}$$

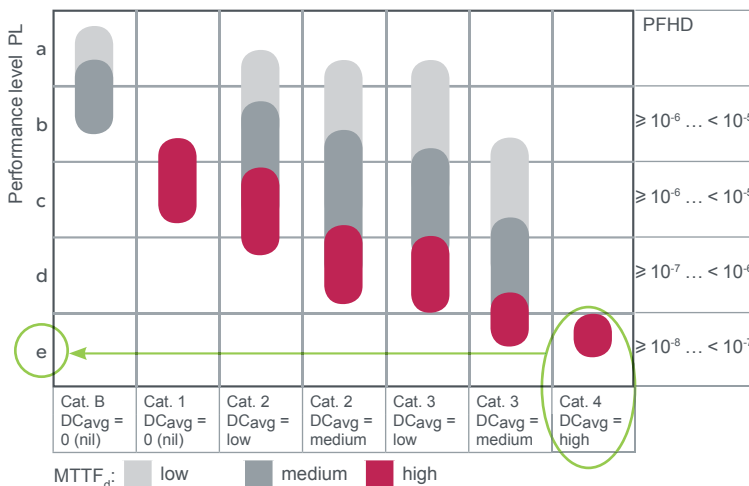
The result of the calculation in our example gives a value of 99%

Stage 5 - Checking that required performance level is achieved

The result of the above calculations is summarised below:

- > a redundant architecture: category 4
- > a mean time to failure > 30 years: high MTTF_d
- > a diagnostic capability of 99%: high DC

Looking at this table, we confirm that **PL level e** is achieved:



Checking the PL

Stage 6 - Validation of the required performance level

The design of SRP/CS must be validated and must show that the combination of SRP/CS performing each safety function satisfies all the applicable requirements of EN/ISO 13849.

Standard EN/IEC 62061
Standards to be applied according to the design selected for the safety-related machine control system

Standard EN/IEC 62061
Machinery safety - Safety-Related Electrical Control systems (SRECS)

Functional Safety of safety-related electrical, electronic and electronic programmable control systems

Field of application of the standard

Safety-related electrical control systems in machines (SRECS) are playing an increasing role in ensuring the overall safety of machines and are more and more frequently using complex electronic technology.

This standard is specific to the machine sector within the framework of EN/IEC 61508. It gives rules for the integration of sub-systems designed in accordance with EN/ISO 13849. It does not specify the operating requirements of non-electrical control components in machines (for example: hydraulic, pneumatic).

Functional approach to safety

As with EN/ISO 13849-1, the process using the EN/IEC 62061 starts with analysis of the risks (EN/ISO 12100) in order to be able to determine the safety requirements.

A particular feature of this standard is that it prompts the user to make a functional analysis of the architecture, then split it into sub-functions and analyse their interactions before deciding on a hardware solution for them (the SRECS).

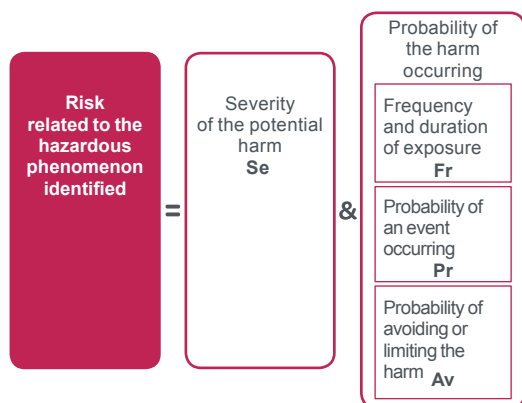
- > A functional safety plan must be drawn up and documented for each design project. It must include:
 - > A specification of the safety requirements for the safety functions (SRCF) that is in two parts:
 - > Description of the functions and interfaces, operating modes, function priorities, frequency of operation, etc.
 - > Specification of the safety integrity requirements for each function, expressed in terms of **SIL** (Safety Integrity Level)
 - > The structured and documented design process for electrical control systems (SRECS)
 - > The procedures and resources for recording and maintaining appropriate information
 - > The process for management and modification of the configuration, taking into account organisation and authorised personnel
 - > The verification and validation plan

> Functional safety

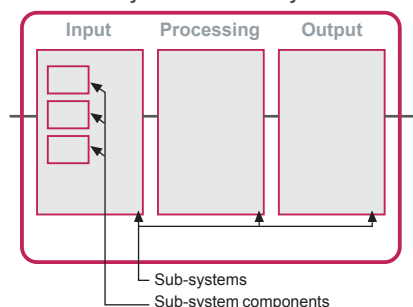
The decisive advantage of this approach is that of being able to offer a failure calculation method that incorporates all the parameters that can affect the reliability of electrical systems, whatever the technology used.

The method consists of assigning a SIL to each function, taking into account the following parameters:

- > The probability of a dangerous failure of the components (PFH_d)
- > The type of architecture; with or without redundancy, with or without diagnostic device making it possible to avoid some of the dangerous failures
- > Common cause failures (power cuts, overvoltage, loss of communication network, etc.) (CCF)
- > The probability of a dangerous transmission error where digital communication is used
- > Electromagnetic interference (EMC)



SRECS: Safety-related control system



Stage 1: Basic structure of the electrical control system

Standard EN/IEC 62061**Machinery safety - Safety-Related Electrical Control systems (SRECS) (continued)****Process**

Designing a system is split into 5 stages after having drawn up the functional safety plan:

- 1** - Based on the safety requirements specification (SRS), assign a safety level (SIL) and identify the basic structure of the electrical control system (SRECS), describe each related function (SRCF)
- 2** - Break down each function into a function block structure (FB)
- 3** - List the safety requirements for each function block and assign the function blocks to the sub-systems within the architecture
- 4** - Select the components for each sub-system
- 5** - Design the diagnostic function and check that the specified safety level (SIL) is achieved.

Stage 1 - Assign a safety integrity level (SIL) and identify the structure of the SRECS

Based on the risk assessment performed in accordance with standard EN/ISO 12100, estimation of the required SIL is performed for each hazardous phenomenon and is broken down into parameters, see illustration opposite.

> Severity Se

The severity of injuries or damage to health can be estimated by taking into account reversible injuries, irreversible injuries and death.

The classification is shown in the table below:

Consequence	Severity Se
Irreversible: death, loss of an eye or an arm	4
Irreversible: shattered limb, loss of a finger	3
Reversible: requires the attention of a medical practitioner	2
Reversible: requires first aid	1

> Probability of the harm occurring

Each of the three parameters Fr, Pr, Av must be estimated separately using the most unfavourable case. It is strongly recommended that a task analysis model be used in order to ensure that estimation of the probability of the harm occurring is correctly taken into account.

> Frequency and duration of exposure Fr

The level of exposure is linked to the need to access the hazardous zone (normal operation, maintenance, ...) and the type of access (manual feeding, adjustment, ...). It must then be possible to estimate the average frequency of exposure and its duration.

The classification is shown in the table below:

Frequency of dangerous exposure	Fr
≤ 1 hour	5
> 1 hour... ≤ 1 day	5
> 1 day... ≤ 2 weeks	4
2 weeks... ≤ 1 year	3
> 1 year	2

> Probability of occurrence of a hazardous event Pr.

Two basic concepts must be taken into account:

- > the predictability of the dangerous components in the various parts of the machine in its various operating modes (normal, maintenance, troubleshooting), paying particular attention to unexpected restarting
- > behaviour of the persons interacting with the machine, such as stress, fatigue, inexperience, etc.

Probability of occurrence of a dangerous event	Pr
Very high	5
Probable	4
Possible	3
Almost impossible	2
Negligible	1

Standard EN/IEC 62061

Standards to be applied according to the design selected for the safety-related machine control system

Standard EN/IEC 62061

Machinery safety - Safety-Related Electrical Control systems (SRECS) (continued)

Process (continued)

Stage 1 -(continued)

> Probability of avoiding or limiting the harm A_v

This parameter is linked to the design of the machine. It takes into account the suddenness of the occurrence of the hazardous event, the nature of the dangerous component (cutting, temperature, electrical) and the possibility for a person to identify a hazardous phenomenon.

Probability of avoiding or limiting the harm	A_v
Impossible	5
Almost impossible	3
Probable	1

> Assignment of the SIL

Estimation is made with the help of the table below.

In our example, the degree of severity is 3 because there is a risk of a finger being amputated; this value is shown in the first column of the table.

All the other parameters must be added together in order to select one of the classes (vertical columns in the table below), which gives us:

- > $Fr = 5$ accessed several times a day
- > $Pr = 4$ hazardous event probable
- > $A_v = 3$ probability of avoiding almost impossible

Therefore a class $CI = 5 + 4 + 3 = 12$

A level of SIL 2 must be achieved by the safety-related electrical control system(s) (SRECS) on the machine.

Estimation of the SIL

Se	Class CI				
	3-4	5-7	8-10	11-13	14-15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3	-	-	SIL 1	SIL 2	SIL 3
2	-	-	-	SIL 1	SIL 2
1	-	-	-	-	SIL 1

> Basic structure of the SRECS

Without going into detail about the hardware components to be used, the system is broken down into sub-systems. In our case, we find the 3 sub-systems that will perform the input, processing and output functions. The figure opposite illustrates this stage, using the terminology given in the standard.

Stage 2 - Break down each function into a function block structure (FB)

A function block (FB) is the result of a detailed break down of a safety-related function.

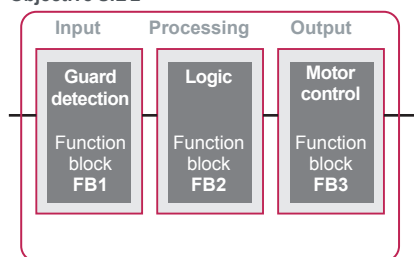
The function block structure gives an initial concept of the SRECS architecture. The safety requirements of each block are deduced from the specification of the safety requirements of the system's function.

Stage 3 - List the safety requirements for each function block and assign the function blocks to the sub-systems within the architecture

Each function block is assigned to a sub-system in the SRECS architecture. A failure of any sub-system will lead to the failure of the safety-related control function. More than one function block may be assigned to each sub-system. Each sub-system may include sub-system elements and, if necessary, diagnostic functions in order to ensure that anomalies can be detected and the appropriate action taken.

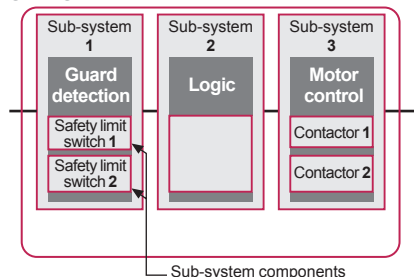
These diagnostic functions (D) are considered as separate functions; they may be performed within the sub-system, by another internal or external sub-system.

SRECS Objective SIL 2



Stage 2: Break down into function blocks

SRECS



Stage 3: Assignment of function blocks

Standard EN/IEC 62061 Machinery safety - Safety-Related Electrical Control systems (SRECS) (continued)

Process (continued)

Stage 4 - Select the components for each sub-system

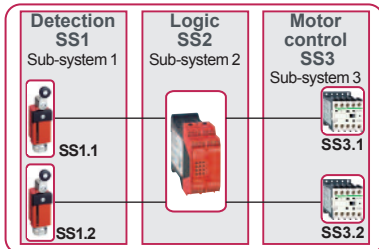
The products shown in the illustration opposite are selected. If the sensors and contactors are the same as in the previous example, a safety module XPS AK will be chosen. In this example, we take a cycle of 450s which means the duty cycle **C** is 8 operations per hour.

As the safety integrity level required for the entire system is SIL 2, each of the components must achieve this level.

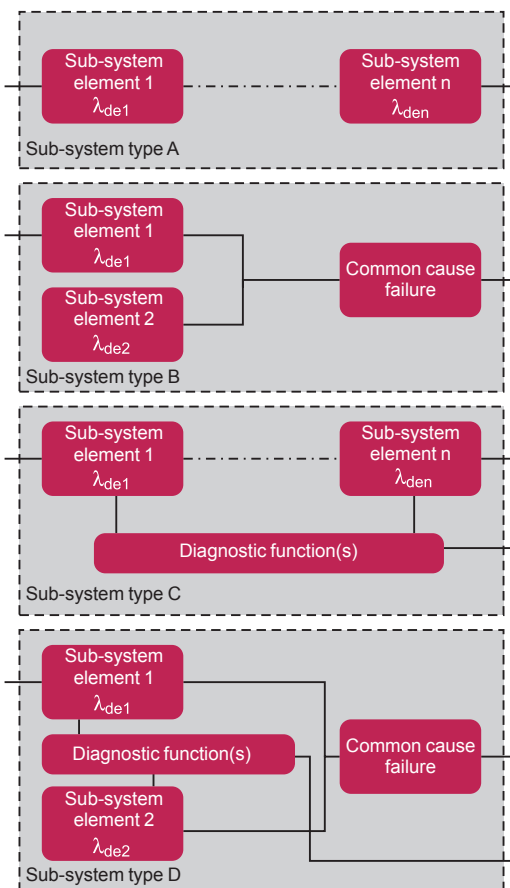
The manufacturer's catalogue gives the following values:

Safety limit switches 1 and 2: $B_{10} = 10\,000\,000$ operations, the proportion of dangerous failures is 20%, lifetime is 10 years.

- > Safety module: $PFH_d = 7.389 \cdot 10^{-9}$
- > Contactors 1 and 2: $B_{10} = 1\,000\,000$ operations, the proportion of dangerous failures = 73%, lifetime is 20 years



Stage 4: Component selection



Types of sub-system architecture

Stage 5 - Design the diagnostic function

The SIL of the sub-system depends not only on the components, but also on the architecture selected. For our example, we will choose architectures B and D of the standard.

In our architecture, the safety module performs diagnostics not only on itself, but also on the safety limit switches.

We have three sub-systems for which the safety levels must be determined:

- > SS1: two redundant safety limit switches in a sub-system with a type D architecture
- > SS2: a SIL 3 safety module (obtained on the basis of the PFH provided by the manufacturer)
- > SS3: two redundant contactors built in accordance with a type B architecture

The calculation method can be found in the machine safety guide, so we will only give the final result. This method takes into account the following parameters:

- > B_{10} : number of operations at which 10% of the population fail
- > **C**: Duty cycle (number of operations per hour)
- > λ_D : rate of dangerous failures ($\lambda_D = \lambda \times$ portion of dangerous failures in %)
- > β : common cause failure coefficient, which is 10 % here and 10% is the worst case: see Annex F
- > **T1**: Proof Test Interval or life time whichever is smaller, as provided by the supplier
- > **T2**: diagnostic test interval
- > **DC**: Diagnostic coverage rate = λ_{DD}/λ_D , ratio between the rate of detected failures and the rate of dangerous failures

We obtain:

- > for SS1 $PFH_d = 1.6 \cdot 10^{-9}$
- > for SS3 $PFH_d = 1.06 \cdot 10^{-7}$

The total probability of dangerous failures per hour is:

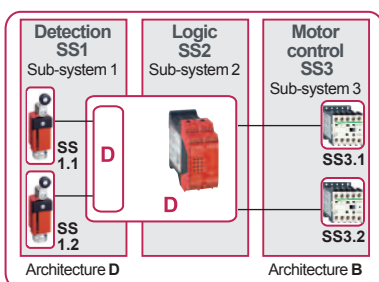
- > $PFH_{DSRECS} = PFH_{DSS1} + PFH_{DSS2} + PFH_{DSS3}$
- > $PFH_{DSRECS} = 1.6 \cdot 10^{-9} + 7.38 \cdot 10^{-9} + 1.06 \cdot 10^{-7} = 1.15 \cdot 10^{-7}$

Which corresponds to the expected result (table below) of a SIL = 2.

Comment: A level of SIL 3 could have been achieved by using mirror contacts to create a feedback loop on the contactors, i.e. a sub-system architecture type D.

Checking the required SIL

SIL	Probability of dangerous failures per hour (PFHd)
3	$\geq 10^{-8} \dots < 10^{-7}$
2	$\geq 10^{-7} \dots < 10^{-6}$
1	$\geq 10^{-6} \dots < 10^{-5}$



Stage 5: Design of the diagnostic function