Safe Machinery Handbook

Schneider Electric

Contents

Introduction

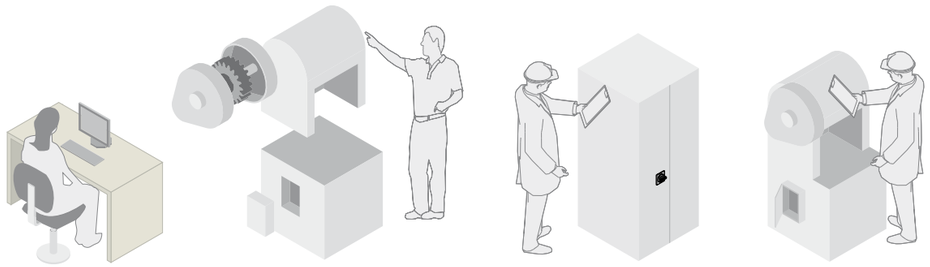
There are various guides to machinery safety legislation which tend to present a distorted view of the requirements of that legislation.

This handbook is an attempt to provide information that is up-to-date and unbiased in order to help machine builders and users to provide workers with machines that are safe, legal, and efficient. It is not intended as an exhaustive guide to compliance with safety legislation, nor as a replacement for referring to the relevant standards themselves; it is to guide you through the logical steps and to point you to the relevant sources of information.

Why safety

As well as the moral obligation to avoid harming anyone, there are laws that require machines to be safe, and sound economic reasons for avoiding accidents.

Safety must be taken into account right from the design stage and must be kept in mind at all stages in the life of a machine: design, manufacture, installation, adjustment, operation, maintenance and eventual scrapping.



Design/manufacture | Installation | Adjustment/operation | Maintenance

New machines - the Machinery Directive

The Machinery Directive 98/37/EC is to compel manufacturers to guarantee a minimum safety level for machineryand equipmentsold within the European Union.

From 29 December 2009 the new Machinery Directive 2006/42/EC will be effective.

Machines have to comply with the Essential Health and Safety Requirements (EHSRs) listed in Annex I of the Directive, thus setting a common minimum level of protection across the EEA (European Economic Area).

Machine manufacturers, or their authorised representatives within the EU, must ensure that the machine is compliant, the Technical File can be made available to the enforcing authorities on request, the CE marking is affixed, and a Declaration of Conformity has been signed, before the machine may be placed on the market within the EU.

Existing machines – the Work Equipment Directive

The user has the obligations defined by the Use of Work Equipment directive 89/655/EEC which can in the most cases be met by using machinery compliant with relevant standard.

It applies to the provision of all work equipment, including mobile and lifting equipment, in all workplaces and work situations.

They require that all equipment is suitable for use, and is inspected and maintained as necessary to ensure that it remains so.

The cost of accidents

Some of the costs are obvious, such as sick pay for injured employees, whereas some costs are harder to identify. The Health and Safety Executive in UK (HSE) give an example of an accident at a drilling machine that resulted in costs to the business of £45 000 (~51 300 €) (HSE INDG355). However this does not include some of the less obvious costs, and some estimates amount to double that figure. An accident analysed by Schneider Electric Ltd, the outcome of which was a reversible head injury, cost the employer some £90 000 (~102 600 €), of which only £37 000 (~42 200 €) was insurable. The full financial impact can include increase in insurance premiums, lost production, lost customers and even loss of reputation.

Some risk reduction measures can actually increase productivity; for example the use of light curtains to protect access points of machines can allow easier access for loading and unloading; zoning of isolation devices can allow parts of a machine to be shut down for maintenance while other parts remain productive.

The regulations apply to all employers, the self-employed, and others who have control of the provision of work equipment.

Legal framework

EC Directive:

- Legal instrument to harmonise the legislation of the European member states
- Defines the essential health and safety requirements (EHSRs)
- Transposed into national law (act, decree, order, regulations)

Standard:

- A “standard” is a technical specification approved by a recognised standardisation body for repeated or continuous application, with which compliance is not compulsory

Harmonised standard:

- A standard becomes harmonised when published throughout the member states

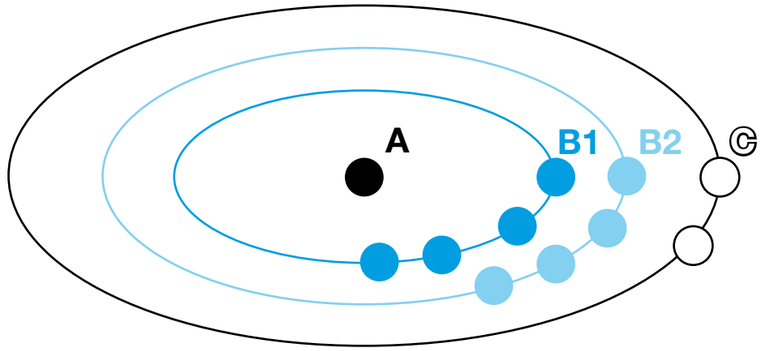
Presumption of conformity:

When a product conforms to a harmonised European standard, the reference to which has been published in the Official Journal of the European Union for a specific Directive, and which covers one or more of the essential safety requirements, the product is presumed to comply with those essential safety requirements of the Directive. A list of such standards can be accessed at http://www.newapproach.org/Directives/DirectiveList.asp

It is of course necessary to ensure compliance with all the other EHSRs as well as those for which a Presumption of Conformity is given by the use of a specific standard.

A B & C standards:

European standards for the Safety of machinery form the following structure:



Type A standards

> (Basic safety standards) giving basic concepts, principles for design, and general aspects that can be applied to all machinery;

Type B standards

> (Generic safety standards) dealing with one safety aspect or one type of safeguard that can be used across a wide range of machinery:

- Type B1 standards on particular safety aspects (e.g. safety distances, surface temperature, noise);
- Type B2 standards on safeguards (e.g. two-hand controls, interlocking devices, pressure sensitive devices, guards);

Type C standards

> (Machine safety standards) dealing with detailed safety requirements for a particular machine or group of machines.

When a Type-C standard deviates from one or more provisions dealt with by a Type A standard or by a Type B standard, the Type C standard takes precedence. PrEN 12100 is Type A standards.

Some examples of these types of standards are:

PrEN/ISO 12100	**A**	Safety of machinery - Principles for risk assessment and risk reduction
EN 574	**B**	Two-hand control devices - Functional aspects - principles for design
EN/ISO 13850	**B**	Emergency stop - Principles for design
EN/IEC 62061	**B**	Functional safety of safety-related electrical, electronic and electronic programmable control systems
EN/ISO 13849-1	**B**	Safety of machinery - Safety-related parts of control systems - Part 1 general principles for design
EN 349	**B**	Minimum gaps to avoid crushing of parts of the human body
EN/SO 13857	**B**	Safety of machinery - Safety distances to prevent hazard zones being reached by upper and lower limbs
EN/IEC 60204-1	**B**	Safety of machinery - Electrical equipment of machines - Part 1: general requirements
EN 999/ISO 13855	**B**	Positioning of protective equipment in respect of approach speeds of parts of the human body
EN 1088/ISO 14119	**B**	Interlocking devices associated with guards - Principles for design and selection
EN/IEC 61496-1	**B**	Electro-sensitive protective equipment Part 1: General requirements and tests
EN/IEC 60947-5-5	**B**	Low-voltage switchgear and control gear - Part 5-5: Control circuit devices and switching elements - Electrical emergency stop device with mechanical latching function
EN 842	**B**	Visual danger signals - General requirements, design and testing
EN 1037	**B**	Prevention of unexpected start-up
EN 953	**B**	General requirements for the design and construction of fixed and movable guards
EN 201	**C**	Machinery for plastics and rubber - Injection moulding machines - Safety requirements
EN 692	**C**	Machine Tools - Mechanical presses - Safety requirements
EN 693	**C**	Machine Tools - Hydraulic presses - Safety requirements
EN 289	**C**	Rubber and plastics machines - Safety - Blow moulding machines intended for the production of hollow articles - Requirements for the design and construction
EN 422	**C**	Blow moulding machines for producing hollow parts - Design and construction requirements
EN/ISO 10218-1	**C**	Robots for industrial environments - Safety requirements - Part 1: Robot
EN 415-4	**C**	Safety of packaging machines - Part 4: palletisers and depalletisers
EN 619	**C**	Continuous handling equipment and systems - Safety and EMC requirements for equipment for mechanical handling of unit loads
EN 620	**C**	Continuous handling equipment and systems - Safety and EMC requirements for fixed belt conveyors for bulk material

Manufacturers' responsibilities

Manufacturers placing machines on the market within the European Economic Area must comply with the requirements of the Machinery Directive. Note that "placing on the market" includes an organisation supplying a machine to itself, i.e. building or modifying machines for its own use, or importing machines into the EEA.

Users' responsibilities

- Users of machines need to ensure that newly-purchased machines are CE marked, and accompanied by a Declaration of Conformity to the Machinery Directive. Machines must be used in accordance with the manufacturer's instructions.

  Existing machines taken into service before the Machinery Directive came into force do not need to comply, although they need to comply with PUWER and be safe and fit for purpose.

- Modification of machines can be considered as manufacture of a new machine, even if for use in-house, and the company modifying a machine needs to be aware that it might need to issue a Declaration of Conformity and CE marking.

Risk assesment

In order for a machine (or other equipment) to be made safe it is necessary to assess the risks that can result from its use. Risk assessment and risk reduction for machines is described in PrEN/ISO 12100.

There are various techniques for risk assessment, and none can be said to be “the right way” to perform a risk assessment. The local Standard specifies some general principles but cannot specify exactly what has to be done in every case. It would seem to be nice if the standard could give a value or ‘score’ for each risk, and then a target value for the maximum value that must not be exceeded, but that is not the case for several reasons. The score that would be allocated to each risk, as well as on the level of risk that can be tolerated, depend on a series of judgements, and will vary with the person doing the judging as well as on the environment. For example the risks that might be reasonable in a factory employing skilled workers might be unacceptable in an environment where members of the public, including children, might be present. Historical accident/incident rates can be useful indicators, but cannot give a reliable indication of accident rates that can be expected.

Identify the limits of the machinery

> That is, just what is being assessed? What are the speeds/loads/substances etc that might be involved? For example how many bottles is the extruder blow moulding per hour, and how much material is being processed at what temperature? Remember to include foreseeable misuse, such as the possible use of a machine outside its specification. What is the expected life of the machinery and its application? How is it likely to be disposed of at the end of its life?

Identify the hazards

> What aspects of the machine might cause harm to a person? Consider the possibility of entanglement, crushing, cutting from tools, sharp edges on the machine or on the material being processed. Other factors such as the stability of the machine, noise, vibration, and emission of substances or radiation also need to be considered, as well as burns from hot surfaces, chemicals, or friction due to high speeds. This stage should include all hazards that can be present during the lifecycle of the machinery, including the construction, installation, and disposal.

Examples of typical hazards are illustrated below, though this is not an exhaustive list. A more detailed list can be found in PrEN/ISO 12100.

Who might be harmed by the identified hazards, and when?

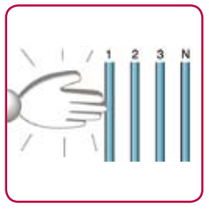
> Who interacts with the machine, when, and why? Again remember foreseeable misuse including the possibility of use of a machine by untrained persons, and persons who might be present in the workplace; not just machine operators, but cleaners, security staff, visitors, and members of the public.

Puncturing, stabbing, shearing, severing, cutting

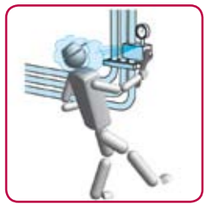
Catching, entanglement, drawing in, trapping

Impact

Crushing



Electrocution



Discharge of dangerous substances

Burns

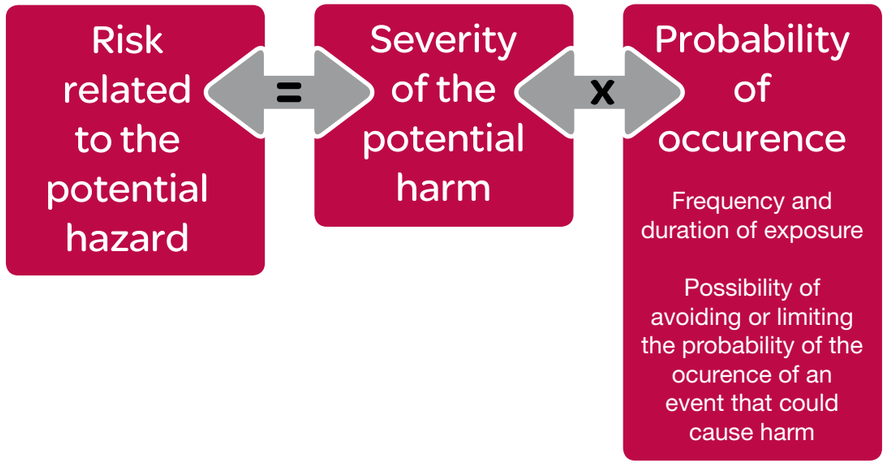
Examples of typical hazards are illustrated here, though this is not an exhaustive list. A more detailed list can be found in PrEN/ISO 12100.

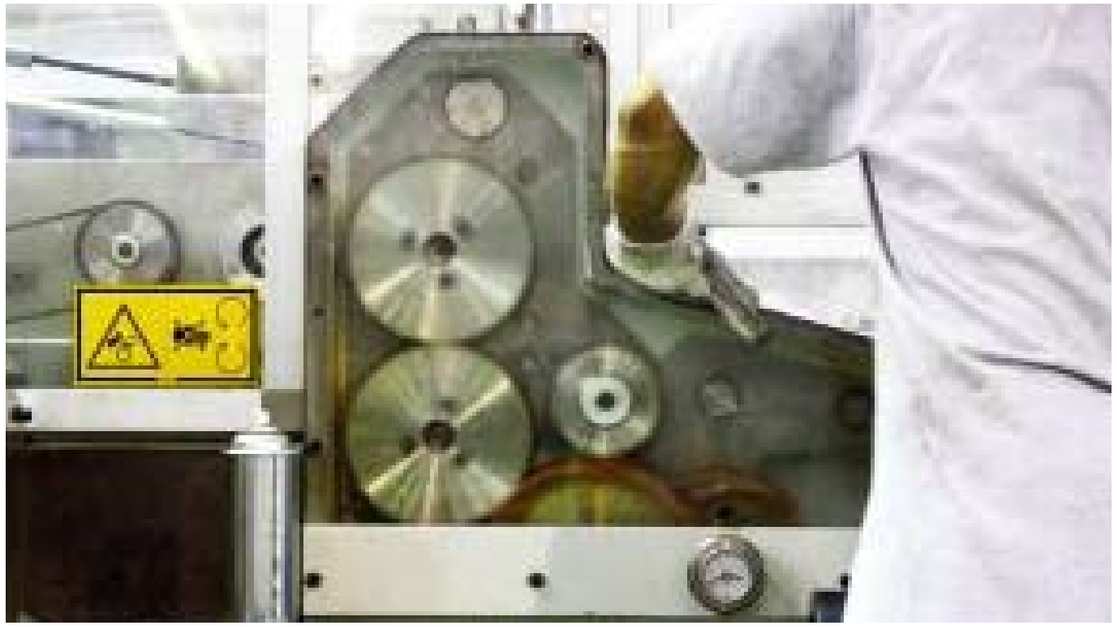
Prioritise the risks according to their seriousness

> PrEN/ISO 12100 describes this stage as Risk Estimation. This can be done by multiplying the potential harm that can come from the hazard by the exposure to the hazard, remembering that there can be more than one person exposed.

It is difficult to estimate the potential harm, given the possibility that every accident can lead to a fatality. However usually when there is more than one possible consequence, one will be more likely than the others. All plausible consequences should be considered, not just the worst case.

The result of the Risk Assessment process should be a table of the various risks that exist at the machine, together with an indication of the seriousness of each. There is not a single “risk rating” or “risk category” for a machine – each risk must be considered separately. Note that the seriousness can only be estimated – Risk Assessment is not a precise science. Neither is it an end in itself; the purpose of Risk Assessment is to guide Risk Reduction.





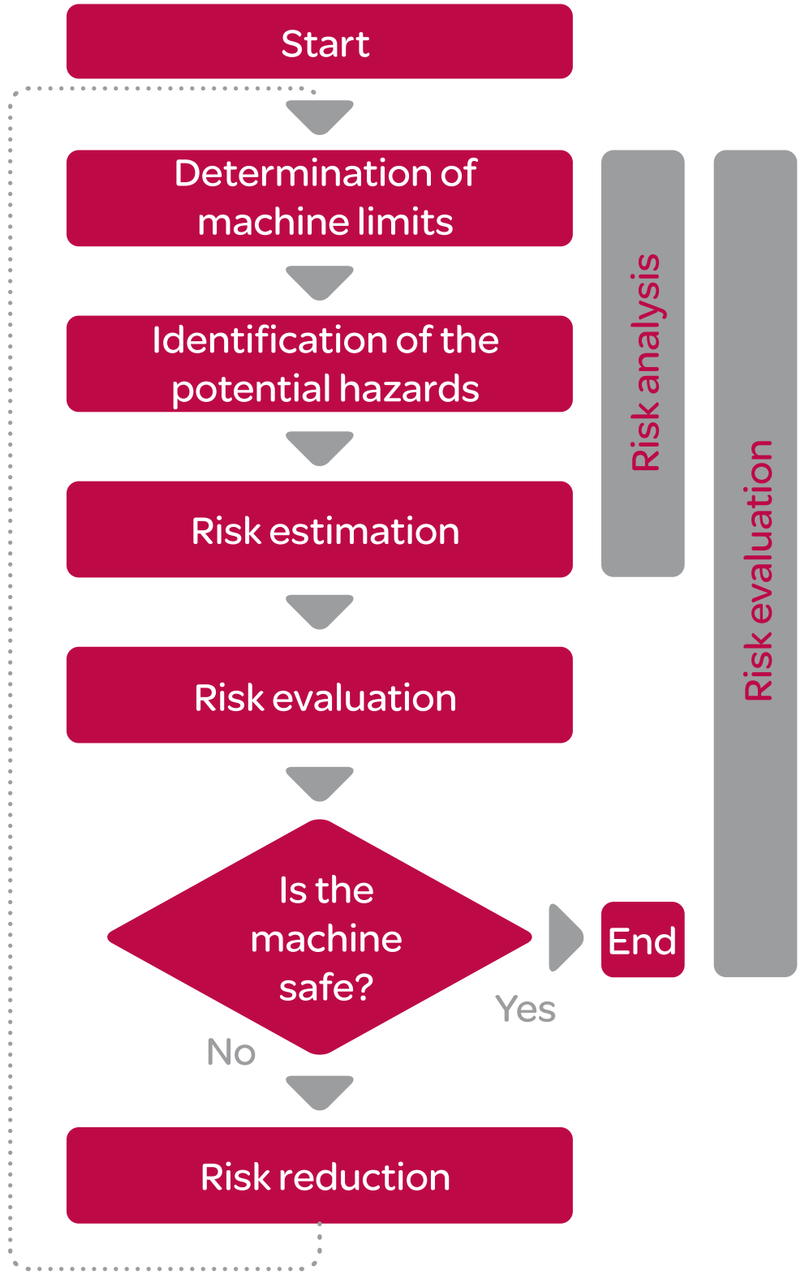
Risk Reduction

> Risk reduction is now included in PrEN/ISO 12100.

Risk reduction is defined in terms of eliminating risk: “the aim of measures taken must be to eliminate any risk throughout the foreseeable lifetime of the machinery including the phases of transport, assembly, dismantling, disabling and scrapping.”

In general, if a risk can be reduced then it should be reduced. This has to be tempered by commercial realities though, and regulations use words like “reasonable” to indicate that it might not be possible to eliminate some risks without a grossly disproportionate cost.

The process of risk assessment is iterative – risks need to be identified, prioritised, quantified, design steps taken to reduce them (first by safe design, then by safeguarding), and then this process is to be repeated to assess whether the individual risks have been reduced to a tolerable level and that no additional risks have be introduced. In the next chapter we examine safe design and safeguarding.

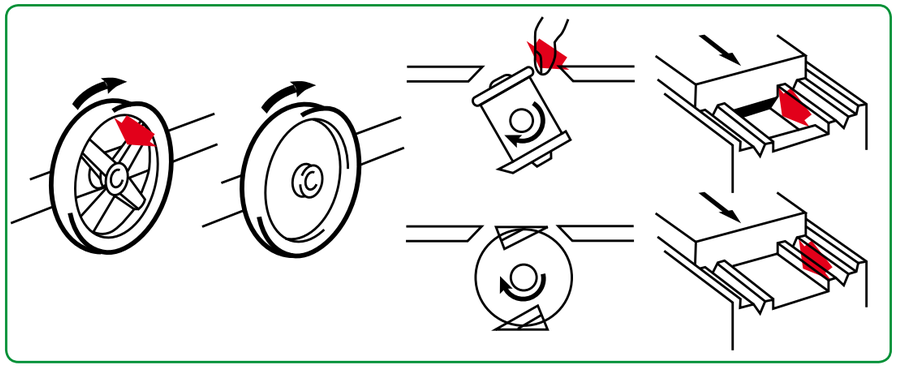


Safe design & safe-guarding

Inherently safe design measures
(as per PrEN/ISO 12100)

> Some risks can be avoided by simple measures; can the task that results in the risk be eliminated? Elimination can sometimes be achieved by automation of some tasks such as machine loading. Can the hazard be removed? For example, the use of a non-flammable solvent for cleaning tasks can remove the fire hazard associated with flammable solvents. This stage is known as **inherently safe design**, and is the only way of **reducing a risk to zero**.

Removing the drive from the end roller of a roller conveyor will reduce the possibility of someone being caught up by the roller. Replacing spoked pulleys with smooth discs can reduce shearing hazards. Avoidance of sharp edges, corners and protusions can help to avoid cuts and bruises. Increasing minimum gaps can help to avoid body parts getting crushed, reducing maximum gaps can eliminate the possibility of body parts entering. Reduced forces, speeds and pressures can reduce the risk of injury.



Removal of shear traps by inherently safe design measures Source: BS PD 5304

> Take care to avoid substituting one hazard for another. For example air-powered tools avoid the hazards associated with electricity, but can introduce other hazards from the use of compressed air, such as injection of air into the body and compressor noise.

Standards and legislation express a distinct hierarchy for controls. The elimination of hazards or reduction of risks to a tolerable level, by inherently safe design measures is the first priority.

Safeguarding & complementary protective measures
(as per PrEN/ISO 12100)

> Where inherently safe design is not practicable, the next step is **safeguarding**. This measure can include, for example, fixed guarding, interlocked guarding, presence sensing to prevent unexpected start-up, etc.

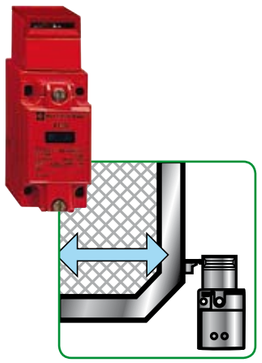
Safeguarding should prevent persons from coming into contact with hazards, or reduce hazards to a safe state, before a person can come into contact with them.

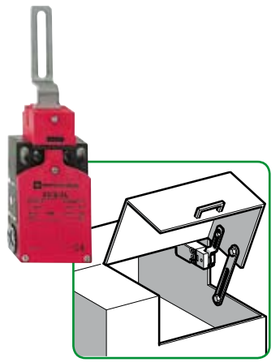
Guards themselves can be fixed to enclose or distance a hazard, or movable such that they are either self-closing, power-operated or interlocked.

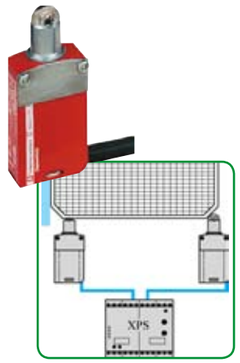
Typical protective devices used as part of safeguarding systems include:

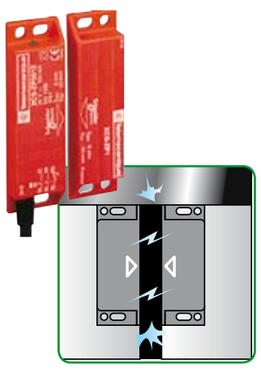
> Interlock switches to detect the position of movable guards for control interlocking, usually to permit tasks such as loading/unloading, cleaning, setting, adjustment etc.

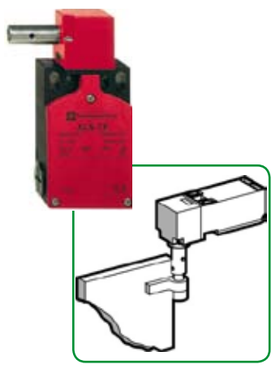
Protection of operators is provided by stopping the machine when the actuator is withdrawn from the head of the switch, when the lever or plunger is actuated, when the guard is opened or the guard hinge rotates through 5° – generally on machines with low inertia (i.e. quick stopping times)







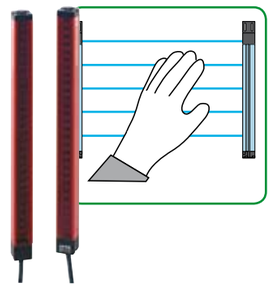




Light curtains to detect approach to dangerous areas

> By finger, hand or body (upto 14mm, upto 30mm and above 30mm resolution)

Light curtains are typically used in material handling, packaging, conveyor, warehousing and other applications. They are designed for the protection of persons operating or working in the vicinity of machinery, by the stopping of dangerous movement of parts as soon as one of the light beams is broken. They make it possible to protect personnel whilst allowing free access to machines. The absence of a door or guard reduces the time taken required for loading, inspection or adjustment operations as well as making access easier.



Safety mats to detect persons

> Approaching, standing in or climbing into the danger area

Safety foot mats are typically used in front of or around potentially dangerous machines or robots. They provide a protection zone between the machine operators and any dangerous movements. They are mainly designed to ensure the safety of personnel, and supplement safety products such as light curtains to enable free access for the loading or unloading of machines. They work by detecting persons stepping onto the mat and instigating a stopping of the dangerous movement.

Solenoid interlocks (powered guards) to prevent opening of guards

> During dangerous phases of operation. Unlike non-solenoid interlocks, they are used on loads with high inertia i.e. where the stopping time is long and it is preferable to permit access only when the dangerous movement has stopped. These are often used with either a time delay circuit (where machine stopping time is defined and known) or actual detection of zero speed (where stopping times can vary) to permit access only when safe conditions are met.

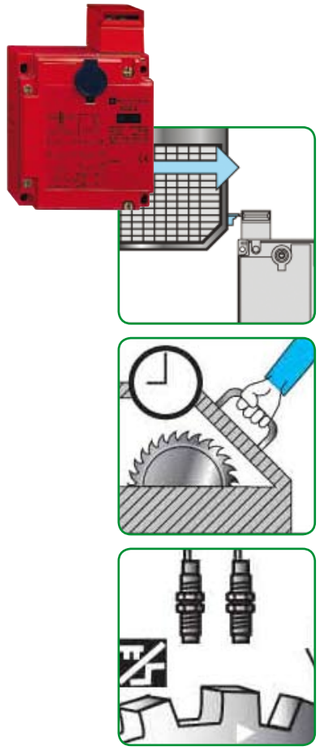
Interlocking devices should be selected and installed with regard to minimising the possibility of defeat and failure, and the overall safeguard should not unnecessarily impede production tasks. Steps to achieve this include:

- devices fastened securely in a (fixed) place and requiring a tool to remove or adjust;

- coded devices or systems, e.g. mechanically, electrically, magnetically or optically;

- physical obstruction or shielding to prevent access to the interlocking device when the guard is open;

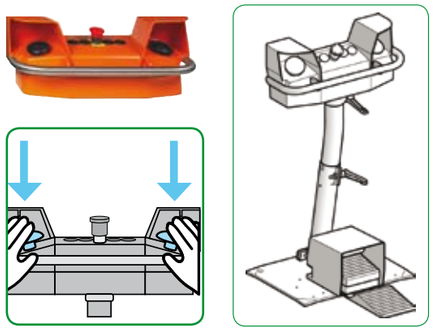
- the support for devices shall be sufficiently rigid to maintain correct operation



Two hand control stations and footswitches

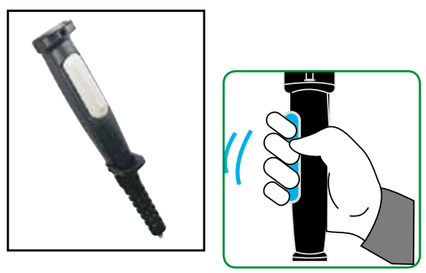
> Used to ensure the operator is standing away from the danger area when causing dangerous movements (e.g. down stroke in press applications)

They provide protection primarily to the machine operator. Supplementary protection to other personnel can be provided through other measures, such as the positioning of light curtains.



Enabling switches to permit access under specific conditions of reduced risk

> To areas for fault-finding, commissioning etc (e.g. jogging and inching), with a central position and 2 “off” positions (fully released or clenched).



Monitoring of safety signals – control systems

> The signals from safeguarding components are typically monitored using safety relays, safety controllers or safety PLCs (collectively referred to as “safety logic solvers”), which in turn are used to drive (and sometimes monitor) output devices such as contactors.

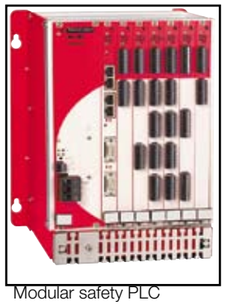
The choice of logic solver will depend upon many factors including the number of safety inputs to process, cost, complexity of the safety functions themselves, the need to reduce cabling through decentralisation using a fieldbus such as AS-Interface Safety at Work or SafeEthernet, or even the need to send safety signals/data over long distances across large machines or between machines on large sites. The now common use of complex electronics and software in safety controllers and safety PLCs has, in part, driven the evolution of the standards relating to safety related electrical control systems.

Two such standards available at time of writing include EN/ISO 13849-1 (directly replacing EN 954-1 the first January 2010) and EN/IEC 62061.

Safety relay

Safety controller

Compact safety PLC



Modular safety PLC

> Safeguarding will usually involve the use of some kind of control system, and the Machinery Directive gives various requirements for the performance of the control system. In particular it states “Control systems must be designed and constructed in such a way as to prevent hazardous situations from arising”. The Machinery Directive does not specify the use of any particular standard, but the use of a control system meeting the requirements of harmonised standard(s) is one means of demonstrating compliance with this requirement of the Machinery Directive. Two such standards available at the time of writing are EN/ISO 13849-1 (replacing EN 954-1 the first January 2010) and EN/IEC 62061.

Complementary protective measures - Emergency stop

Although emergency stops are required for all machines (the Machinery Directive allows two very specific exemptions) they are not considered to be a primary means of risk reduction. Instead they are referred to as a “complementary protective measure”. They are provided as a **backup for use in an emergency only**. They need to be robust, dependable, and available at all positions where it might be necessary to operate them.

EN/IEC 60204-1 defines the following three categories of stop functions as follows:

– Stop category 0: stopping by immediate removal of power to the machine actuators (uncontrolled stop);

– Stop category 1: a controlled stop with power available to the machine actuators to achieve the stop and then removal of power when the stop is achieved;

– Stop category 2: a controlled stop with power left available to the machine actuators.

However stop category 2 is not usually considered suitable for emergency stops.

Emergency stops on machinery must be “trigger action”. This means that their design ensures that however slowly the button is pressed, or cable pulled, if the normally-closed contact opens the mechanism must latch. This prevents “teasing”, which can cause dangerous situations. The converse must also be true, i.e. latching must not take place unless the NC contact opens. Emergency stop devices should comply with EN/IEC 60947-5-5.

Residual risks

After risks have been reduced as far as possible by design, and then by safeguarding, the risk assessment process should be repeated to check that no new risks have been introduced (e.g. powered guards can introduce trapping hazards) and to estimate whether each risk has been reduced to a tolerable level. Even after some iterations of the risk assessment/risk reduction procedure, it is likely that there will be some residual risks.

Except for machines built to a specific harmonised standard (C Standard) it is for the designer to judge whether the residual risk is tolerable or whether further measures need to be taken, and to provide information about those residual risks, in the form of warning labels, instructions for use, etc. The instructions might also specify measures such as the need for personal protective equipment (PPE) or special working procedures, but these are not as dependable as measures implemented by the designer.

Functional safety

Functional Safety

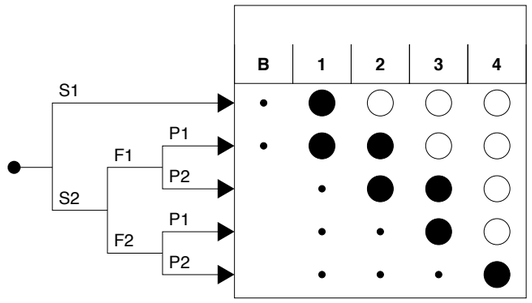
> The IEC have published a series of FAQs related to Functional Safety at http://www.iec.ch/zone/fsafety/

A number of standards have been published in recent years that use the concept of functional safety. Examples include IEC 61508, IEC 62061, IEC 61511, ISO 13849-1, and IEC 61800-5-2 which have all been adopted in Europe and published as ENs.

Functional safety is a relatively recent concept that replaces the old ‘Categories’ of behaviour under fault conditions that were defined in EN 954-1, and were often mistakenly described as ‘Safety Categories’.

A reminder of the principles of EN 954-1

> Users of EN 954-1 will be familiar with the old “risk graph” which many used to design their safety related parts of electrical control circuits to the categories B, 1, 2, 3 or 4. The user was prompted to subjectively assess severity of injury, frequency of exposure and possibility of avoidance in terms of slight to serious, rare to frequent, and possible to virtually impossible, to arrive at a required category for each safety related part.



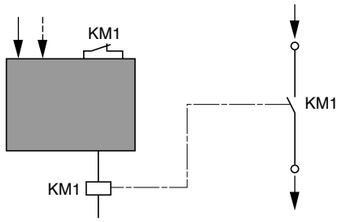
> The thinking is that the more the risk reduction depends upon the safety machine control system* (SRECS), the more it needs to be resistant to faults (such as short circuits, welded contacts etc).

The behaviour of the categories under fault conditions was defined as follows:

- Category B control circuits are basic and can lead to a loss of the safety function due to a fault.

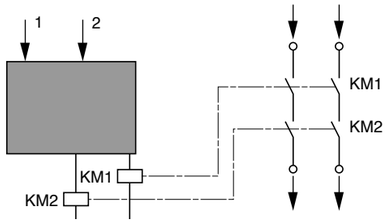
- Category 1 can also lead to a loss of the safety function, but with less probability than category B.

- Category 2 circuits detect faults by periodic testing at suitable intervals (the safety function can be lost between the periodic tests)

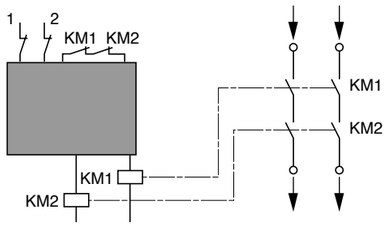


*The safety machine control system is named:
- SRP/CS safety related parts of control system in EN/ISO 13849-1 standard
- SRECS Safety related electrical control system in EN/IEC 62061 standard

- Category 3 circuits ensure the safety function, in the presence of a single fault, for example by employing two (redundant) channels, but a loss of the safety function can occur in the case of an accumulation of faults



- Category 4 circuits ensure that the safety function is always available even in the case of one or more faults, usually by employing both input and output redundancy, together with a feedback loop for continuous monitoring of the outputs



Functional safety is **“part of the overall safety relating to the EUC* and the EUC control system which depends on the correct functioning of the E/E/PE** safety-related systems, other technology safety-related systems and external risk reduction facilities”**. Note that it is an attribute of the equipment under control and of the control system, not of any particular component or specific kind of device. It applies to all components that contribute to the performance of a safety function, including for example, input switches, logic solvers such as PLCs and IPCs (including their software and firmware) and output devices such as contactors and variable speed drives.

* EUC means Equipment Under Control
**Note E/E/PE means Electrical/Electronic/Programmable Electronic.

It should also be remembered that the words “correct functioning” mean that the function is correct, not just what was expected, which means **the functions have to be selected correctly**. In the past there has been a tendency for components specified to a high category of EN 954-1 to be chosen instead of components that have a lower category, but might actually have more suitable functions. This might be as a result of the misconception that the categories are hierarchical such that for example, category 3 is always “better” than category 2 and so on. Functional safety standards are intended to encourage designers to focus more on the functions that are necessary to reduce each individual risk, and what performance is required for each function, rather than simply relying on particular components.

Which standards are applicable to the safety function?

Now that EN 954-1 is about to be withdrawn, the available alternatives are EN/IEC 62061 and EN/ISO 13849-1.

The performance of each safety function is specified as either a SIL (Safety Integrity Level) in the case of EN/IEC 62061 or PL (Performance Level) in the case of EN/ISO 13849-1.

In both cases the architecture of the control circuit which delivers the safety function is a factor, but unlike EN 954-1 these new standards require consideration of the reliability of the selected components.

EN/IEC 62061

It is important to consider each function in detail; EN/IEC 62061 requires a Safety Requirements Specification (SRS) to be drawn up. This includes a functional specification (what it does, in detail) and a safety integrity specification, which defines the required probability that the function will be performed under the specified conditions.

An example often used is “stop the machine when the guard is open”, which really needs more detailed consideration, initially of the functional specification. For example, will the machine be stopped by removing the coil voltage from a contactor, or by ramping-down the speed using a variable speed drive? Is it necessary to lock the guard closed until the dangerous movements have stopped? Will other equipment, upstream or downstream, need to be shut down? How will the opening of the guard be detected?

The safety integrity specification must consider both random hardware failures and systematic failures. Systematic failures are those which are related to a specific cause, and can only be avoided by removal of that cause, usually by a modification of the design. In practice, most ‘real-world’ failures are systematic and result from incorrect specification.

As part of the normal design processes, this specification should lead to the selection of suitable design measures; for example, heavy and misaligned guards can lead to damaged interlock switches unless shock absorbers and alignment pins are fitted, contactors should be suitably rated and protected against overloads.

How often will the guard be opened? What might be the consequences of a failure of the function? What will the ambient conditions (temperature, vibration, humidity, etc) be?

In EN/IEC 62061, a safety integrity requirement is expressed as a target failure value for the probability of dangerous failure per hour of each Safety related control function (SRCF). This can be calculated from reliability data for each component or sub-system, and is related to the SIL as shown in Table 3 of the standard:

Safety integrity level (SIL)	Probability of a dangerous Failure per Hour PFH_D
3	$>10^{-8}$ to $<10^{-7}$
2	$>10^{-7}$ to $<10^{-6}$
1	$>10^{-6}$ to $<10^{-5}$

Table 1: Relationship between SIL and PFH_D

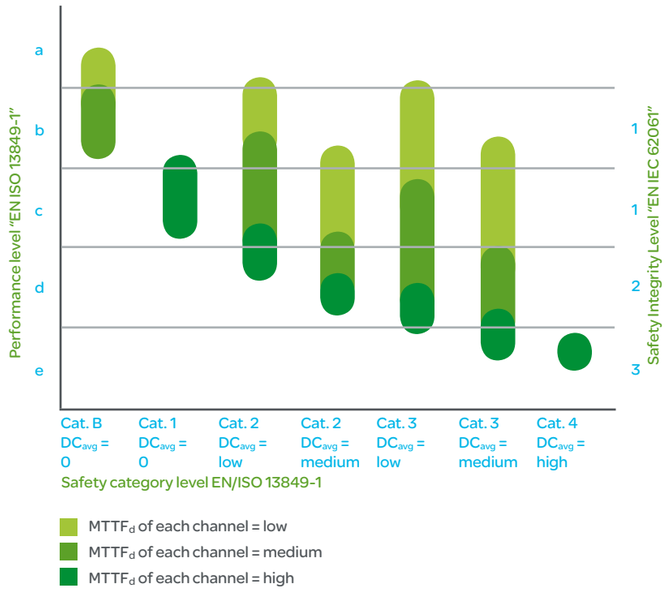
EN ISO 13849-1

EN ISO 13849-1 uses a combination of the Mean Time To Dangerous Failure ($MTTF_d$), Diagnostic Coverage (DC) and architecture (category) to determine Performance Level PL (a, b, c, d, e), and a simplified method of estimating PL is given in Table 7 of the standard. The categories are the same as those in EN 954-1, which are explained in Annex 2.

Category	B	1	2	2	3	3	4
DC_{avg}	None	None	Low	Medium	Low	Medium	High
$MTTF_d$ of each channel							
Low	a	Not covered	a	b	b	c	Not covered
Medium	b	Not covered	b	c	c	d	Not covered
High	Not covered	c	c	d	d	d	e

Table 2: Simplified procedure for evaluating PL achieved by SRP/CS

From the table above it can be seen that only a category 4 architecture can be used to achieve the highest PLe, but that is possible to achieve lower PLs using categories depending upon the mix of $MTTF_d$ and DC of the components used.



Index	MTTFd range
Low	>3 years to <10 years
Medium	>10 years to <30 years
High	>30 years to <100 years

Table 3: MTTFd levels

- For the estimation of $MTTF_d$ of a component the following data can be used, in order of preference:

  1. Manufacturer's data ($MTTF_d$, B10 or $B10_d$)
  2. Methods in Annexes C and D of EN/ISO 13849-1
  3. Choose 10 years

- Diagnostic coverage is a measure of how many dangerous failures the diagnostic system will detect. The level of safety can be increased where sub-systems are tested internally using self-diagnostics.

Index	Diagnostic coverage
Nil	<60%
Low	>60% to <90%
Medium	>90% to <99%
High	>99%

Table 4: Diagnostic Coverage levels

- Common Cause Failures (CCF) is when an external effect (such as physical damage) renders a number of components unusable irrespective of MTTFd. Steps taken to reduce CCF include:

  - Diversity in the components used and modes in which they are driven
  - Protection against pollution
  - Separation
  - Improved electromagnetic compatibility

Which standard to use?

- Unless a C-standard specifies a target SIL or PL, the designer is free to choose whether to use EN/IEC 62061 or EN/ISO 13849-1, or indeed any other standard. Both EN/IEC 62061 and EN/ISO 13849-1 are harmonised standards that give a Presumption of Conformity to the Essential Requirements of the Machinery Directive, in so far as they apply. However it should be remembered that whichever standard is chosen must be used in its entirety, and they cannot be mixed in a single system.

  Work is ongoing in a liaison group between IEC and ISO, to produce a common Annex for the two standards with the aim of eventually producing a single standard.

  EN/IEC 62061 is perhaps more comprehensive on the subjects of specification and management responsibilities, whereas EN/ISO 13849-1 is designed to allow an easier transition from EN 954-1.

Certification

- Some component products are available with certification to a specific SIL or PL. It should be remembered that these certificates are only an indication of the best SIL or PL that can be achieved by a system using that component in a specific configuration, and are not a guarantee that a completed system will meet any specific SIL or PL.

Control system standards worked examples

Perhaps the best way to understand the application of EN/IEC 62061 and EN/ISO 13849-1 is by way of the worked examples on the following pages.

For both standards we will use the example where the opening of a guard must cause the moving parts of a machine to stop, where if it did not stop the resulting possible injury could be a broken arm or amputated finger.

Worked example using standard EN/IEC 62061

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

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 13849-1. It does not specify the operating requirements of non-electrical control components in machines (for example: hydraulic, pneumatic).

Functional approach to safety

The process starts with analysis of the risks (PrEN/ISO 12100) in order to be able to determine the safety requirements. A particular feature of EN/IEC 62061 is that it prompts the user to make an analysis of the architecture to perform the safety functions, then consider sub-functions and analyse their interactions before deciding on a hardware solution for the safety control system called safety related electrical control system (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:

- A 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).

- Table 1 below gives the target maximum failure values for each SIL.

Safety integrity level SIL	Probability of a dangerous Failure per Hour, PFH_D
3	$>10^{-8}$ to $<10^{-7}$
2	$>10^{-7}$ to $<10^{-6}$
1	$>10^{-6}$ to $<10^{-5}$

- 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.

The advantage of this approach is that it can offer a calculation method that incorporates all the parameters that can affect the reliability of control systems. 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 (A, B, C or D), i.e.;
  With or without redundancy,
  With or without diagnostic features making it possible to control some of the dangerous failures,

- Common cause failures (CCF), including;
  Short-circuits between channels,
  Overvoltage,
  Loss of power supply, etc.,

- The probability of dangerous transmission errors where digital communication is used,

- Electromagnetic interference (EMI).

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

1. Based on the risk assessment, assign a safety integrity 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,

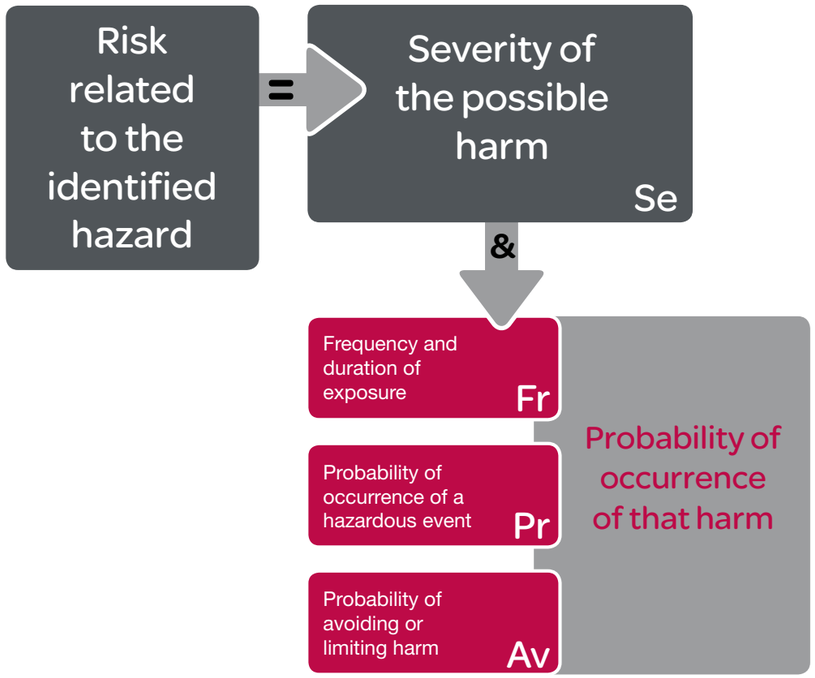
4. Select the components for each sub-system,

5. Design the diagnostic function and check that the specified safety integrity level (SIL) is achieved.

In our example, consider a function which removes the power to a motor when a guard is opened. If the function fails, it would be possible for the machine operator's arm to be broken or a finger amputated.

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

> Based on the risk assessment performed in accordance with PrEN/ISO 12100, estimation of the required SIL is performed for each safety-related control function (SRCF) and is broken down into parameters, as shown in the illustration below.



Severity Se

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

The recommended classification is shown in the table below.

Consequences	Severity (Se)
Irreversible: death, losing an eye or arm	4
Irreversible: broken limb(s), losing a finger(s)	3
Reversible: requiring attention from a medical practitioner	2
Reversible: requiring first aid	1

Probability of the harm occurring

> Each of the three parameters Fr, Pr, Av is estimated separately using the least favourable case. It is recommended that a task analysis is 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 is then possible to estimate the average frequency and duration of exposure.

The recommended classification is shown in the table below:

Frequency of exposure	Duration > 10 min
< 1 h	5
> 1 h to < 1 day	5
> 1 day to < 2 weeks	4
> 2 weeks to < 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	Probability (Pr)
Very high	5
Likely	4
Possible	3
Rarely	2
Negligible	1

Probability of avoiding or limiting the harm Av

> 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 hazard (cutting, temperature, electrical), the possibility of physically avoiding the hazard, and the possibility for a person to identify a hazardous phenomenon.

Probabilities of avoiding or limiting harm (AV)	
Impossible	5
Rarely	3
Probable	1

SIL assignment:

> Estimation is made with the help of the table below.

In our example, the degree of severity (Se) 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:

Fr = 5 accessed several times a day
Pr = 4 hazardous event probable
Av = 3 probability of avoiding almost impossible

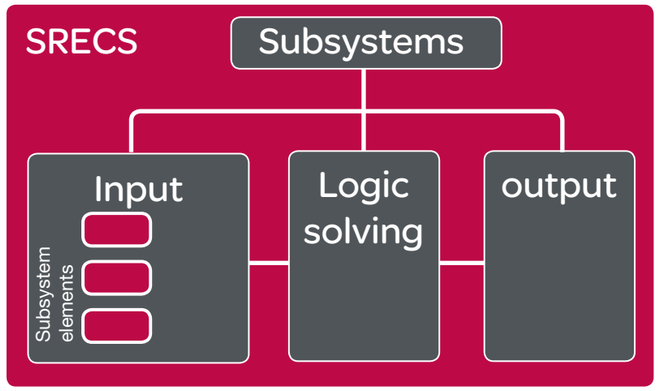
Therefore a class **Cl = 5 + 4 + 3 = 12**

The safety-related electrical control system (SRECS) of the machine must perform this function with an integrity level of SIL 2.

Severity (Se)	Class (Cl)				
	3-4	5-7	8-10	11-13	14-15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3		(OM)	SIL 1	SIL 2	SIL 3
2			(OM)	SIL 1	SIL 2
1				(OM)	SIL 1

Basic structure of the SRECS

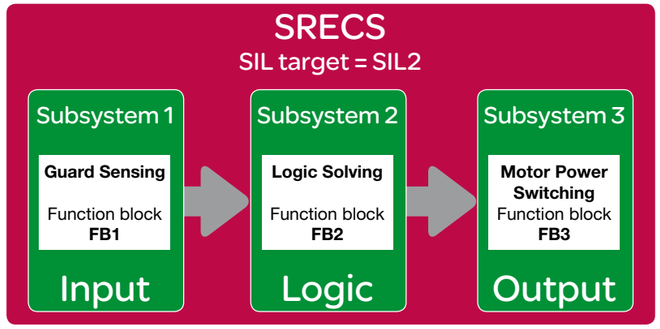
> Before going into detail about the hardware components to be used, the system is broken down into sub-systems. In this example, 3 sub-systems are necessary to perform the input, processing and output functions. The figure opposite illustrates this stage, using the terminology given in the standard.



Step 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.

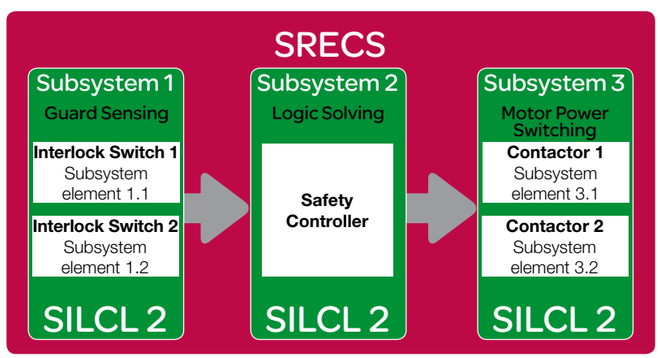
The function block structure gives an initial concept of the SRECS architecture. The safety requirements of each block are derived from the safety requirements specification of the corresponding safety-related control function.



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

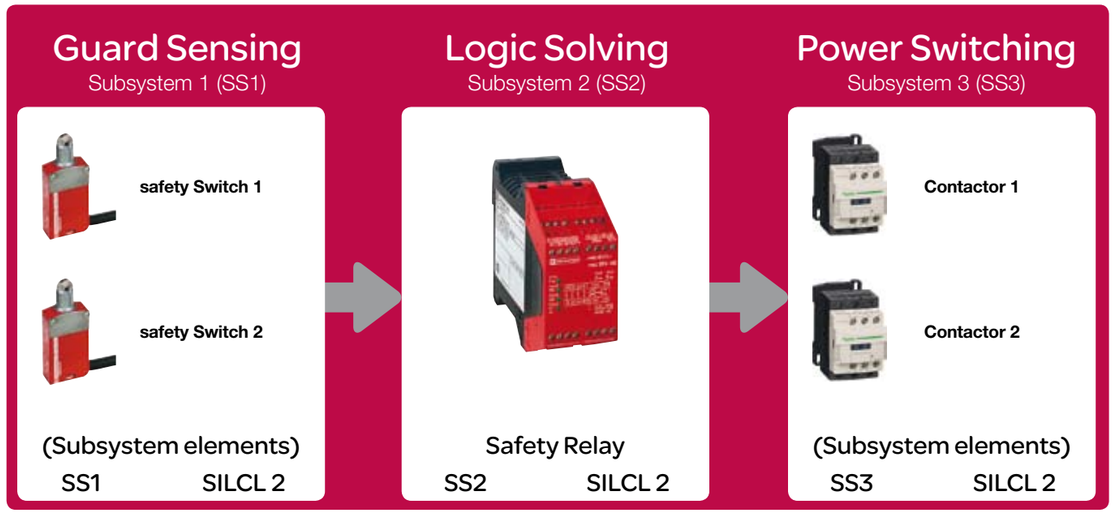
> Each function block is assigned to a sub-system in the SRECS architecture. (The standard defines 'subsystem' in such a way that failure of any sub-system will lead to the failure of a safety-related control function.) More than one function block may be assigned to each sub-system. Each sub-system may include sub-system elements and, if necessary, diagnostic functions in order to ensure that failures can be detected and the appropriate action taken.

These diagnostic functions are considered as separate functions; they may be performed within the sub-system, or by another sub-system. The sub-systems must achieve at least the same SIL capability as assigned to the entire safety-related control function, each with its own SIL Claim Limit (SILCL). In this case the SILCL of each subsystem must be 2.



Step 4 - Select the components for each sub-system

> The products shown below are selected.



Component	Number of operations (B10)	% dangerous failures	Lifetime
XCS safety limit switches	10 000 000	20%	10 years
XPS AK safety logic module	$PFH_D = 7.389 \times 10^{-9}$		
LC1 TeSys contactor	1 000 000	73%	20 years

The reliability data is obtained from the manufacturer.

The cycle length in this example is 450 seconds, so the duty cycle **C** is 8 operations per hour, i.e. the guard will be opened 8 times per hour.

Step 5 - Design the diagnostic function

> The SIL achieved by the sub-systems depends not only on the components, but also on the architecture selected. For this example, we will choose architectures B for the contactor outputs and D for the limit switch (See Annex 1 of this Guide for explanation of architectures A, B, C and D).

In this architecture, the safety logic module performs self-diagnostics, and also checks the safety limit switches. There are three sub-systems for which the SILCLs (SIL Claim Limits) must be determined:

SS1: two safety limit switches in a sub-system with a type D (redundant) architecture;
SS2: a SILCL 3 safety logic module (determined from the data, including PFH_D, provided by the manufacturer);
SS3: two contactors used in accordance with a type B (redundant with no feedback) architecture

The calculation takes into account the following parameters:

B10: number of operations at which 10% of the population will have failed.
C: Duty cycle (number of operations per hour).

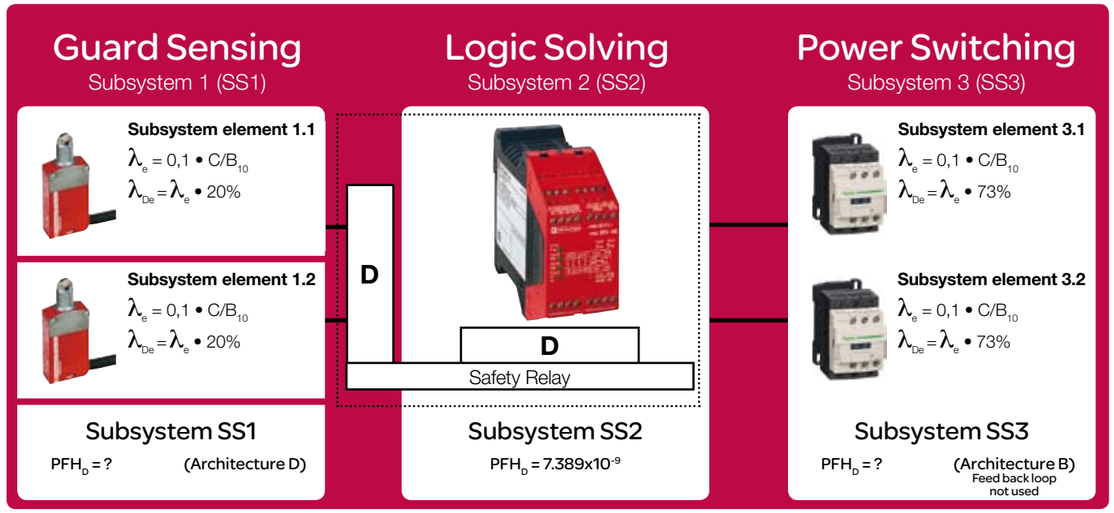
λ_D: rate of dangerous failures (λ = x proportion of dangerous failures).

β: common cause failure factor: see Annex F of the standard.

T1: Proof Test Interval or life time, whichever is smaller, as specified by the manufacturer. The standard states that designers should use a lifetime of 20 years, to avoid the use of an unrealistically short proof test interval being use to improve the SIL calculation. However it recognises that electromechanical components can need replacement when their specified number of operations is reached. Therefore the figure used for T1 can be the manufacturer's quoted lifetime, or in the case of electromechanical components the $B10_D$ value divided by the rate of operations C.

T2: diagnostic test interval.

DC: Diagnostic coverage rate = $\lambda_{DD} / \lambda_{Dtotal}$, the ratio between the rate of detected dangerous failures and the rate of total dangerous failures.



> The failure rate, λ, of an electromechanical subsystem element is defined as $\lambda e = 0,1 \times C / B10$, where C is the number of operations per hour in the application and B10 is the expected number of operations at which 10% of the population will have failed. In this example we will consider C = 8 operations per hour.

			SS1 2 monitored limit switches	SS3 2 contactors without diagnostics
Failure rate for each element λ_e	λ_e = 0.1 C/B_{10}			
Dangerous failure rate for each element λ_{De}	$\lambda_{De} = \lambda_e$ x proportion of dangerous failures			
DC			99%	Not Applicable
Common cause failure factor β			Assumed worst case of 10%	
T1 min (life time B10d/C)	T1 = B_{10d}/C		(10 000 000/20%)/8 = 87 600	(10 000 000/73%)/8 = 171 232
Diagnostic test interval T2			Each demand, i.e. 8 times per hour, = 1/8 = 0.125 h	Not applicable
Dangerous failure rate for each subsystem	Formula for architecture B: $\lambda_{DssB} = (1-\beta)^2 \times \lambda_{De1} \times \lambda_{De2} \times T1 + \beta \times (\lambda_{De1} + \lambda_{De2})/2$	Formula for architecture D $\lambda_{DssD} = (1-\beta)^2 \{[\lambda_{De2} \times {}^2 \times DC] \times T_2/2 + [\lambda_{De2} \times (1-DC)] \times T_1\} + \beta \times \lambda_{De}$		$\lambda_{DssB} = (1-0.9)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + \beta \times (\lambda_{De1} + \lambda_{De2})/2$

Looking at the output contactors in subsystem SS3 we need to calculate the PFH_d. For the type B architecture (single fault tolerant, without diagnostics) the probability of dangerous failure of the subsystem is:

$\lambda_{DssB} = (1 - \beta)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + \beta \times (\lambda_{De1} + \lambda_{De2})/2$
[Equation B of the standard]

$PFHDssB = \lambda_{DssB} \times 1h$

In this example, $\beta = 0.1$
$\lambda_{De1} = \lambda_{De2} = 0.73\ (0.1 \times C / 1\ 000\ 000) = 0.73(0.8/1\ 000\ 000) = 5.84 \times 10^{-7}$
$T1 = \min(\text{life time}, B10_D/C) = \min(175\ 200^*, 171\ 232) = 171\ 232$ hours
* Life time 20 years min 175 200 hours

$\lambda_{DssB} = (1 - 0.1)^2 \times 5.84 \times 10^{-7} \times 5.84 \times 10^{-7} \times 171\ 232 + 0.1 \times ((5.84 \times 10^{-7}) + (5.84 \times 10^{-7}))/2$

$= 0.81 \times 5.84 \times 10^{-7} \times 5.84 \times 10^{-7} \times 171\ 232 + 0.1 \times 5.84 \times 10^{-7}$
$= 0.81 \times 3.41056 \times 10^{-13} \times 171\ 232 + 0.1 \times 5.84 \times 10^{-7}$
$= (3.453 \times 10^{-8}) + (5.84 \times 10^{-8}) = 1.06 \times 10^{-7}$
Since $PFH_{DssB} = \lambda_{DssB} \times 1h$, PFH_D for the contactors in Subsystem SS3 = 1.06×10^{-7}

For the input limit switches in Subsystem SS1 we need to calculate the PFH_D. For the Type D architecture, single fault tolerance with diagnostic function is defined.
This architecture is such that a single failure of any subsystem element does not cause a loss of the SRCF, where

T_2 is the diagnostic test interval;
T_1 is the proof test interval or lifetime whichever is the smaller.
β is the susceptibility to common cause failures;$\lambda_D = \lambda_{DD} + \lambda_{DU}$; where λ_{DD} is the rate of detectable dangerous failures and λ_{DU} is the rate of undetectable dangerous failure.
$\lambda_{DD} = \lambda_D \times DC$
$\lambda_{DU} = \lambda_D \times (1 - DC)$
For subsystem elements of the same design:
λ_{De} is the dangerous failure rate of a subsystem element;
DC is the diagnostic coverage of a subsystem element.

$\lambda_{DssD} = (1 - \beta)^2 \{[\lambda_{De}^2 \times 2 \times DC] \times T_2/2 + [\lambda_{De}^2 \times (1 - DC)] \times T_1\} + \beta \times \lambda_{De}$

D.2 of the standard
$PFH_{DssD} = \lambda_{DssD} \times 1h$
$\lambda_e = 0{,}1 \bullet C / B10 = 0.1 \times 8/10\ 000\ 000 = 8 \times 10^{-8}$
$\lambda_{De} = \lambda_e \times 0.2 = 1.6 \times 10^{-8}$
DC = 99%
β = 10% (worst case)
$T_1 = \min(\text{life time}, B10_D/C) = \min[87600^*, (10\ 000\ 000/20\%)] = 87\ 600$ hours
$T_2 = 1/C = 1/8 = 0.125$ hour
* Life time 10 years min 87 600 hours

From D.2:
$\lambda_{DssD} = (1 - 0.1)^2 \{[1.6 \times 10^{-8} \times 1.6 \times 10^{-8} \times 2 \times 0.99] \times 0.125/2 + [1.6 \times 10\text{-}8 \times 1.6 \times 10^{-8} \times (1 - 0.99)] \times 87\ 600\} + 0.1 \times 1.6 \times 10^{-8}$

$= 0.81 \times \{[5.0688 \times 10^{-16}] \times 0.0625 + [2.56 \times 10\text{-}16 \times (0.01)] \times 87\ 600\} + 1.6 \times 10^{-9}$
$= 0.81 \times \{3.168 \times 10^{-17} + [2.56 \times 10\text{-}18] \times 87\ 600\} + 1.6 \times 10^{-9}$
$= 1.82\ 10^{-13}$
$= 1.6 \times 10^{-9}$
Since $PFH_{DssD} = \lambda_{DssD} \times 1h$, PFHD for the limit switches in Subsystem SS1 = 1.63×10^{-9}

We already know that for Subsystem SS2, PFH_D for the logic solver Function Block (implemented by the safety relay XPSAK) is 7.389×10^{-9} (manufacturer's data)
The overall PFH_D for the safety related electrical control system (SRECS) is the sum of the PFH_Ds for all the Function Blocks, and is therefore:
$PFH_{DSRECS} = PFH_{DSS1} + PFH_{DSS2} + PFH_{DSS3} =$
$1.6\ 10^{-9} + 7.389\ 10^{-9} + 1.06\ 10^{-7}$
$= 1.15 \times 10^{-7}$, which by referring to the table below from the standard, is within the limits of SIL 2.

Safety integrity level	Probability of a dangerous Failure per Hour, PFH_D
3	$>10^{-8}$ to $<10^{-7}$
2	$>10^{-7}$ to $<10^{-6}$
1	$>10^{-6}$ to $<10^{-5}$

Note that if the mirror contacts on the contactors are used the architecture of the power control function would become type D (redundant with feedback) and the resulting SIL claim limit would increase from SIL2 to SIL 3.

This provides further risk reduction of the probability of failure of the safety function, being in tune with the concept of reducing risk to be as low as reasonably practical (ALARP)

LC1D TeSys contactors feature mirror contacts

Worked example using standard EN/ISO 13849-1

Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design

> As with EN/IEC 62061, the process can be considered to comprise a series of 6 logical steps.

STEP 1: Risk Assessment and identification of the necessary safety functions.

STEP 2: Determine the required Performance Level (PLr) for each safety function.

STEP 3: Identify the combination of safety-related parts which carry out the safety function.

STEP 4: Evaluate the Performance Level PL for the all safety-related parts.

STEP 5: Verify that the PL of the SRP/CS* for the safety function is at least equal to the PLr.

STEP 6: Validate that all requirements are met (see EN/ISO 13849-2).

*Safety related part of control system (name of safety machine control system in EN/ISO 13849-1 standard).

For more detail please refer to Annex 2 of this Guide.

> STEP 1: As in the previous example, we need a safety function to remove the power supply to the motor when the guard is open.

> STEP 2: Using the “risk graph” from Figure A.1 of EN/ISO 13849-1, and the same parameters as in the previous example, the required Performance Level is d (note: PL=d is often compared to SIL 2 as “equivalent”).

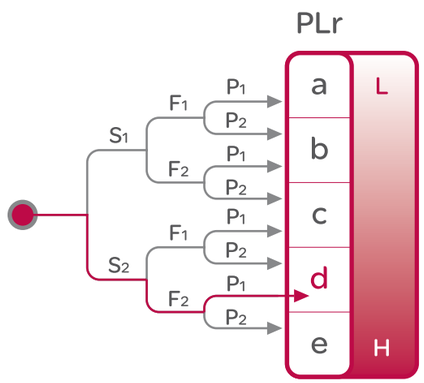
H = High contribution to reduction of the risk by the control system

L = Low contribution to reduction of the risk by the control system

S = Severity of injury
S1 = Slight (normally reversible injury)
S2 = Serious (normally irreversible injury including death)

F = Frequency and/or exposure time to the hazard
F1 = seldom or less often and/or the exposure time is short
F2 = frequent to continuous and/or the exposure time is long

P = Possibility of avoiding the hazard or limiting the harm
P1 = possible under specific conditions
P2 = scarcely possible



> STEP 3: The same basic architecture as in the previous example for EN/IEC 62061 will be considered, in other words category 3 architecture without feedback

> STEP 4: The PL of the SRP/CS is determined by estimation of the following parameters: (see Annex 2):

- The CATEGORY (structure) (see Clause 6 of EN/ISO 13849-1). Note that in this example the use of a category 3 architecture means that the mirror contacts on the contactors are not used.

- The $MTTF_d$ for the single components (see Annexes C & D of EN/ISO 13849-1)

- The Diagnostic Coverage (see Annex E of EN/ISO 13849-1)

- The Common Cause Failures (see score table in Annex F of EN/ISO 13849-1)

> The manufacturer gives the following data for the components:

Example SRP/CS	B10 (operations)	$MTTF_d$ (years)	DC
Safety limit switches	10 000 000		99%
Safety logic module XPSAK		154.5	99%
Contactors	1 000 000		0%

> Note that because the manufacturer does not know the application details, and specifically the cycle rate of the electromechanical devices, he can only give B10 or $B10_d$ data for the electromechanical components. This explains why no manufacturer should provide an $MTTF_d$ figure for an electromechanical device.

> The $MTTF_d$ for components can be determined from the formula:

$MTTF_d = B10d / (0.1 \times n_{op})$

Where n_{op} is the mean annual number of operations.

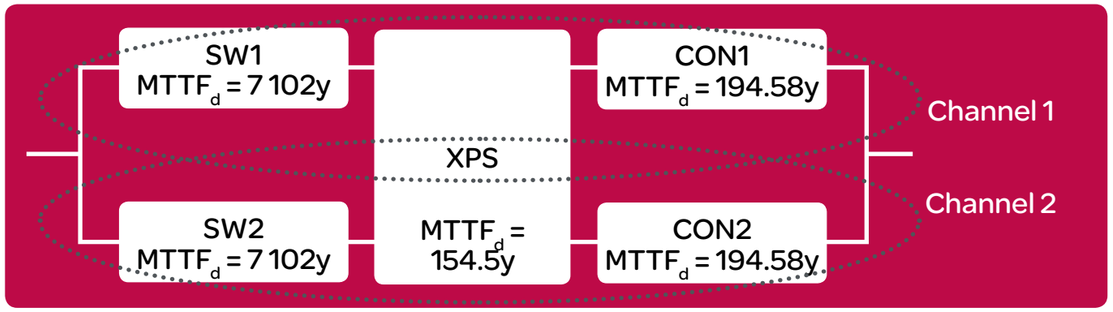
B10 is number of operations at which 10% of the population will have failed.
B10d is the expected time at which 10% of the population will have failed in a “dangerous” mode. Without specific knowledge of which mode in which a component is being used, and hence what constitutes a dangerous failure, for a limit switch the % of dangerous failure is 20%, therefore $B10_d = B10/20\%$
Assuming the machine is used for 8 hours a day, for 220 days per year, with a cycle time of 90 seconds as before, n_{op} will be 70400 operations per year.

> Assuming that B10d = B10/20%, the table becomes:

Example SRP/CS	B10 (operations)	B10d	MTTFd (years)	DC
Safety limit switches	10 000 000	50 000 000	**7 102**	99%
Safety logic module XPSAK			154.5	99%
Contactors	1 000 000	1 369 863	**194.58**	0%

> The $MTTF_d$ figures in bold red have been derived from the application data using the cycle rates and B10 data.

The $MTTF_d$ can be calculated for each channel by using the parts count method in Annex D of the standard.



In this example the calculation is identical for channels 1 and 2:

$$\frac{1}{\text{MTTFd}} = \frac{1}{7\,102 \text{ years}} + \frac{1}{154.5 \text{ years}} + \frac{1}{194.58 \text{ years}} = \frac{1}{85.09 \text{ years}}$$

> The $MTTF_d$ for each channel is therefore 85 years; this is “high” according to Table 3

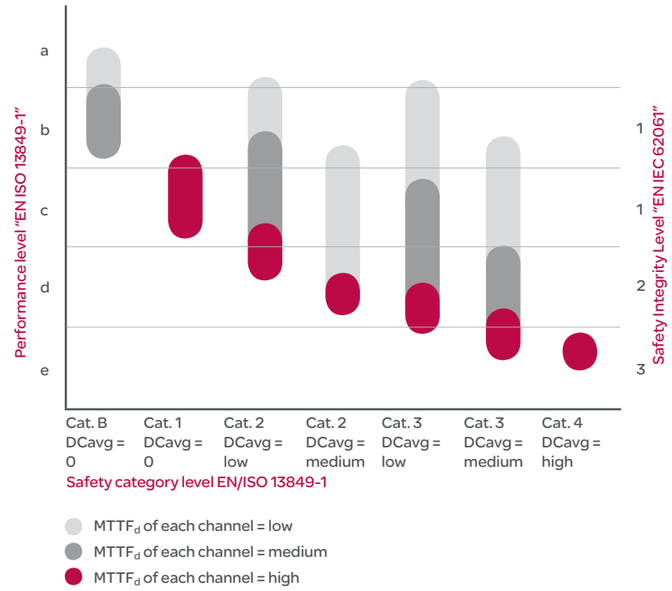
From the equations in Annex E of the standard we can determine that DC_{avg} = 55.7%

> STEP 5: Verify that the PL of the system matches the required PL (PLr)

Knowing that we have a category 3 architecture, a high $MTTF_d$ and a low average Diagnostic Coverage (DC_{avg}), it can be seen from the table below (fig. 5 of the standard) that we have met PL=d, which meets the required PL=d.

Just as in the EN/IEC 62061 worked example, it only takes the wiring of both contactors’ normally closed auxiliary mirror contacts back to the external device monitoring input of the safety relay to change the architecture to category 4. Doing this converts the PL from d to e.

Knowing that we have a category 4 architecture, a high $MTTF_d$ and a high average Diagnostic Coverage (DC_{avg}), referring to Table 7 of the standard shows that the resulting Performance Level is PL=e, which matches the PLr.



> STEP 6: Validation – check working and where necessary test (EN/ISO 13849-2 under revision).

Sources of information

Legislation

- European Machinery Directive 2006/42/EC
- PrEN/ISO 12100 Safety of machinery – principles of risk assessment and risk reduction
- PD 5304:2005 Guidance on safe use of machinery
- EN/IEC 60204 Safety of machinery. Electrical equipment of machines. General requirements
- EN/IEC 13850 Safety of machinery. Emergency stop. Principles for design
- EN/IEC 62061 Safety of machinery, Functional safety of safety-related electrical, electronic and programmable electronic control systems
- EN/IEC 61508 Functional safety of electrical/electronic/programmable electronic safety - related systems
- EN/ISO 13849-1 Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design

Schneider Electric documents

- Schneider Electric “Safety Functions and solutions using Preventa” Catalogue 2008/9, Ref. MKTED208051EN

Schneider Electric documents

Schneider Electric documents

- www.oem.schneider-electric.com

Annexes - architectures

Annex 1

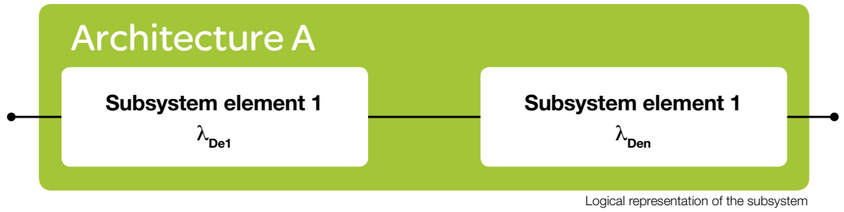
Architectures of EN/IEC 62061

> Architecture A: Zero fault tolerance, no diagnostic function

Where: λ_{De} is the rate of dangerous failure of the element

$$\lambda_{DSSA} = \lambda_{DE1} + \ldots + \lambda_{Den}$$

$$PFH_{DSSA} = \lambda_{DSSA} \bullet 1h$$



Logical representation of the subsystem

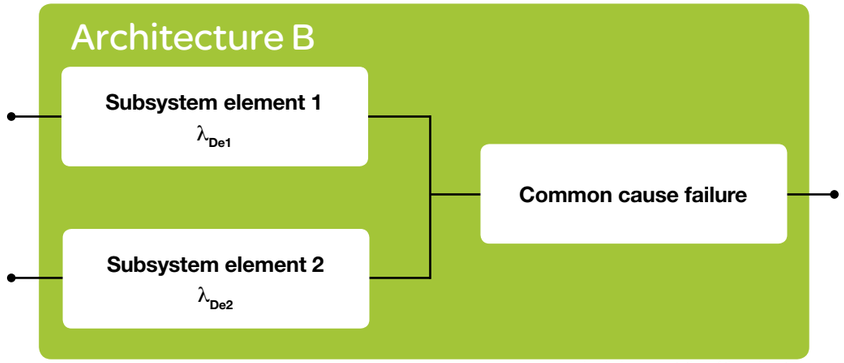
> Architecture B: Single fault tolerance, no diagnostic function

Where: T_1 is the proof test interval or life time whichever is smaller
(Either from the supplier or calculate for electromechanical product by: $T_1 = B_{10}/C$)

β is the susceptibility to common cause failures
(β is determined using the Score Table F.1 from EN/IEC 62061)

$$\lambda_{DSSB} = (1 - \beta)^2 \bullet \lambda_{De1} \bullet \lambda_{De2} \bullet T_1 + \beta \bullet (\lambda_{De1} + \lambda_{De2})/2$$

$$PFH_{DSSB} = \lambda_{DSSB} \bullet 1h$$



Logical representation of the subsystem

> Architecture C: Zero fault tolerance, with a diagnostic function

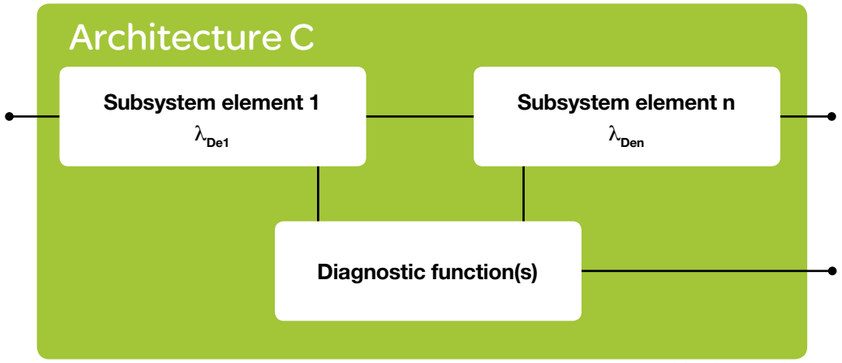
Where: DC is the diagnostic coverage = $\Sigma\ \lambda_{DD}/\lambda_D$

λ_{DD} is the rate of detected dangerous failure and λ_D is the rate of total dangerous failure

The DC depends on the effectivity of the diagnostic function used in this subsystem

$$\lambda_{DSSC} = \lambda_{De1} \bullet (1 - DC_1) + \ldots + \lambda_{Den} \bullet (1 - DC_n)$$

$$PFH_{DSSC} = \lambda_{DSSC} \bullet 1h$$



Logical representation of the subsystem

> Architecture D: Single fault tolerance, with a diagnostic function

Where: T_1 is the proof test interval or life time whichever is smaller

T_2 is the diagnostic test interval

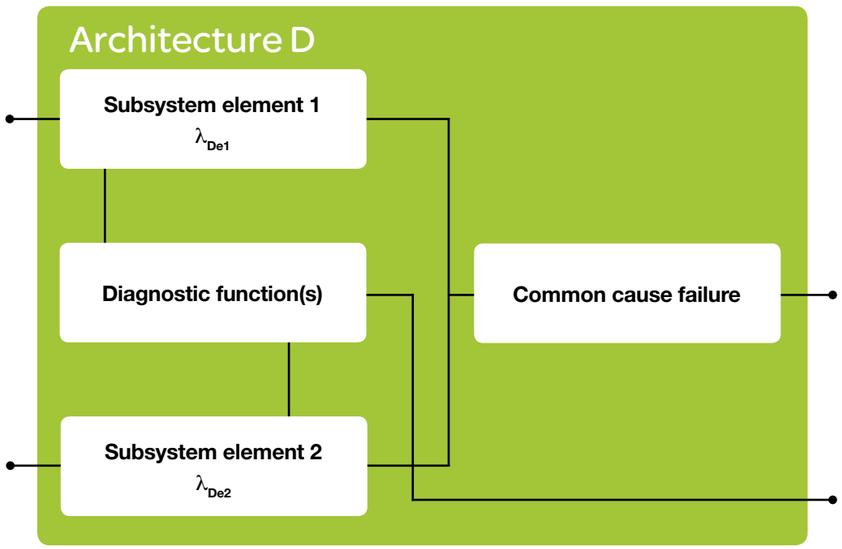
(At least equal to the time between the demands of the safety function)

β is the susceptibility to common cause failures

(To be determined with the score table in Annex F of EN/IEC 62061)

DC is the diagnostic coverage = $\Sigma\ \lambda_{DD}/\lambda_D$

(λ_{DD} is the rate of the detected dangerous failure and λ_D is the rate of the total dangerous failure)



Logical representation of the subsystem

> Architecture D: Single fault tolerance, with a diagnostic function

For Subsystem elements of different design

λ_{De1} = dangerous failure rate of subsystem element 1; DC_1 = diagnostic coverage of subsystem element 1

λ_{De2} = dangerous failure rate of subsystem element 2; DC_2 = diagnostic coverage of subsystem element 2

$$\lambda_{DSSD} = (1-\beta)^2\ \{[\lambda_{De1} \bullet \lambda_{De2}\ (DC_1 + DC_2)] \bullet T_2/2 + [\lambda_{De1} \bullet \lambda_{De2} \bullet (2-DC_1-DC_2)] \bullet T_1/2\} + \beta \bullet (\lambda_{De1} + \lambda_{De2})/2$$

$$PFH_{DSSD} = \lambda_{DSSD} \bullet 1h$$

For Subsystem elements of the same design

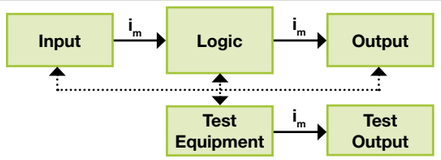
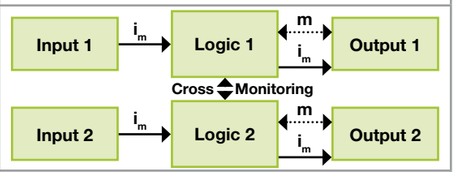
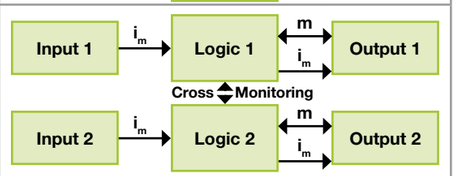
λ_{De} = dangerous failure rate of subsystem element 1 or 2; DC = diagnostic coverage of the subsystem element 1 or 2

$$\lambda_{DSSD} = (1-\beta)^2\ \{[\lambda_{De}^{\ 2} \bullet 2 \bullet DC]\ T_2/2 + [\lambda_{De}^{\ 2} \bullet (1-DC)] \bullet T_1\} + \beta \bullet \lambda_{De}$$

$$PFH_{DSSD} = \lambda_{DSSD} \bullet 1h$$

Annex 2

Categories of EN/ISO 13849-1

Category	Description	Example
Category B	When a fault occurs it can lead to the loss of the safety function	
Category 1	When a fault occurs it can lead to the loss of the safety function, but the $MTTF_d$ of each channel in Category 1 is higher than in Category B. Consequently the loss of the safety function is less likely.	
Category 2	Category 2 system behaviour allows that: 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.	
Category 3	SRP/CS to Category 3 shall be designed so that a single fault in any of these safety-related parts does not lead to the loss of the safety function. Whenever reasonably possible the single fault shall be detected at or before the next demand upon the safety function	
Category 4	SRP/CS to Category 4 shall be designed so that a single fault in any of these safety-related parts does not lead to the loss of the safety function, and the single fault is detected on or before the next demand upon the safety functions, e.g. immediately, at switch on, at end of a machine operation cycle. If this detection is not possible an accumulation of undetected faults shall not lead to the loss of the safety function.	

Schneider Electric Industries SAS

Head Office
35, rue Joseph Monier – CS 30323
F92506 Rueil-Malmaison Cedex
FRANCE

www.schneider-electric.com

ART. 837703

Due to evolution of standards and equipment, characteristics indicated in the text and images in this document are not binding only after confirmation by our departments.

Design: BlueLoft
Photos: Schneider Electric
Print:

11 / 2009

DIA4ED1100102EN