Preventa solutions for efficient machine safety

Safety Legislation and Standards

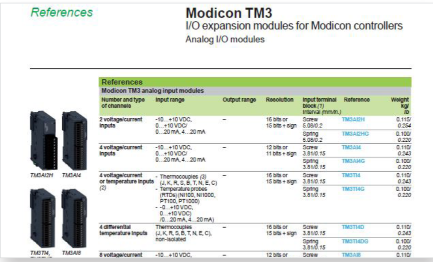
Catalogue

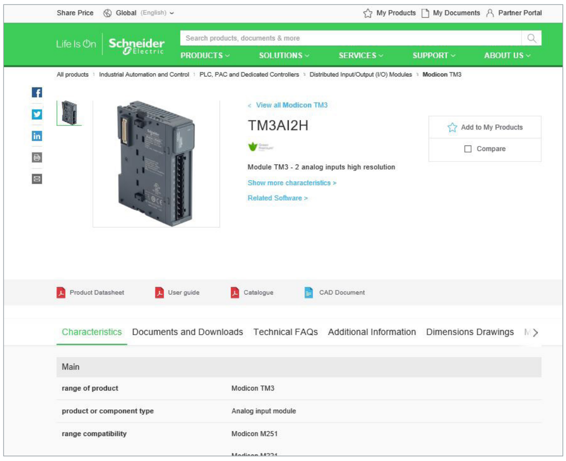
January 2015

Schneider Electric

Quick access to product information

Get technical information about your product

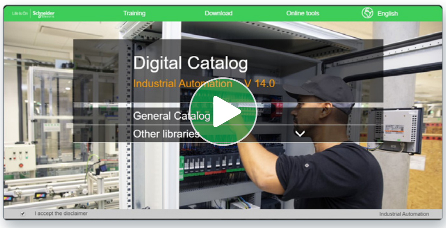




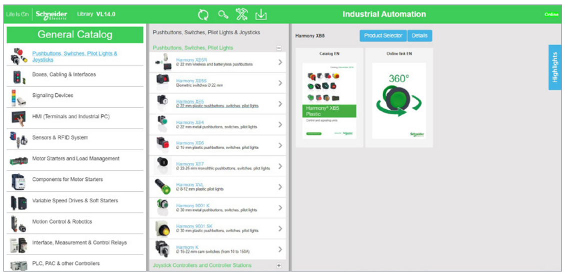
Each commercial reference presented in a catalog contains a hyperlink. Click on it to obtain the technical information of the product:

- Characteristics, Dimensions and drawings, Mounting and clearance, Connections and schemas, Performance curves
- Product image, Instruction sheet, User guide, Product certifications, End of life manual

Find your catalog



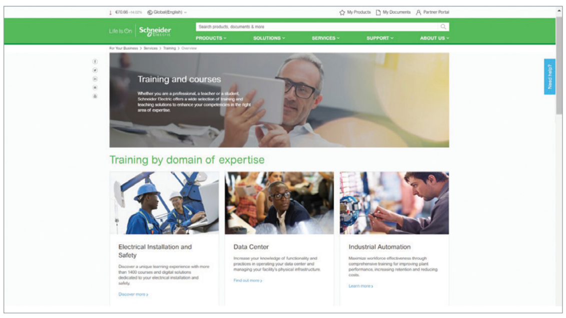
> With just 3 clicks, you can access the Industrial Automation and Control catalogs, in both English and French
> Consult digital automation catalogs at Digi-Cat Online



- Up-to-date catalogs
- Embeded product selectors,360° pictures
- Optimized search by commercial references

Select your training

> Find the right Training for your needs on our Global website
> Locate the training center with the selector tool, using this link



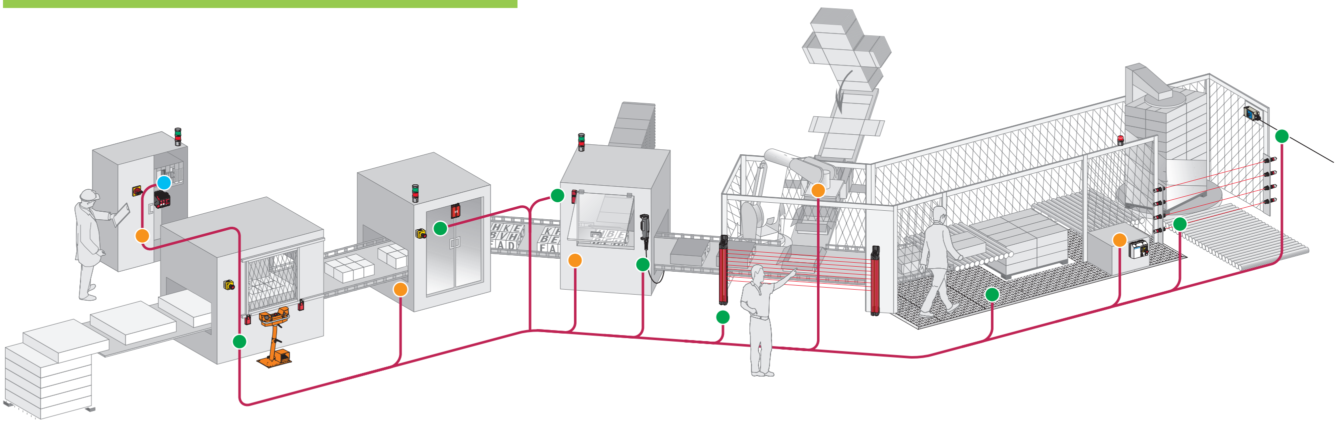
Life Is On Schneider Electric

General contents

Safety Legislation and Standards

Schneider Electric Safety Approach

Product Approach



Schneider Electric is one provider of the complete safety chain.
In addition to moral obligation and economic consequences, the law requires that machinery operates safely in the interests of accident prevention. Preventa offers an extensive range of safety products, compliant with international standards, designed to provide the most comprehensive protection for personnel and equipment.

Aquire the information

- Generic protective measures - Emergency stop
- Two hand control stations and enabling switches for starting and enabling of dangerous movements
- Protective guard devices used as part of safeguarding systems to control the access under specific conditions of reduced risk
- Light curtains to detect approach to dangerous and limited areas

Monitor and processing

- Safety modules manage one safety function, monitoring inputs from safety devices and managing the outputs to contactors and drives
- Safety controllers: configurable safety device capable of managing multiple safety functions simultaneously
- Safety PLCs: programmable electronic systems for complex distributed safety applications

Stop the machine

- Contactors to cut-off the electrical power supply to the motors with mechanically linked mirror auxiliary contacts integrated for the feedback loop diagnosis used by the safety modules, controller and PLCs
- Variable speed drives and servo drives provide controlled stopping of the machine by using embedded safety functions
- Rotary switch disconnectors: for equipment isolation from the electrical supply and for emergency stop by direct interruption of the power supply

Safety Legislation and Standards
Schneider Electric safety approach

Schneider Electric Safety Approach

Solution Approach

One provider for the complete safety chain
- Emergency stop
- Perimeter guarding
- Guard monitoring
- Enabling movement
- Speed monitoring
- Position monitoring

The Safety Chain Solutions are TüV certified safety architectures based upon the most common safety functions required on and around a machine. The safety chain solutions enable you to save time and costs when designing and manufacturing your machine in accordance with the European Machinery Directive.

Each solution comes with:
- Bill of materials and the system description file
- Wiring diagram
- Layout of solution indicating performance level (PL) and safety integrity level (SIL)
- Description of the Performance Level and Safety Integrity Level calculation for the safety function
- Sistema Library file with corresponding solution
- TüV certification

Safety Legislation and Standards
Service we provide

Machine Solutions Services & Support

Service and support that are behind you all the way

Design

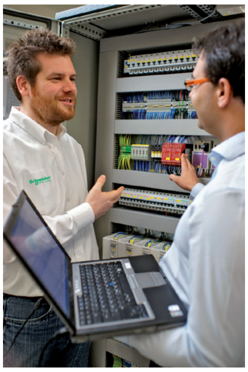
We find the best solution for your needs
- Based on your needs, System and Architecture Experts and Application Design Experts (SAE/ADE) work out innovative technical solutions including
  - Co-engineering
  - Tests
  - Validation

We understand your pain points
- Consulting

We execute the solution with a full service agreement
- Our solution design and project centers (Flex-Centres) are committed to quality and results and provide:
  - Project and program management
  - Software and hardware engineering
  - Tests, validation, and commissioning

We improve your team's competencies
- In class training and on site training

Build



We ensure the delivery of your solution
- Availability of components through a large worldwide network of distributors
- Collaboration, management, and delivery through local partners
- With Schneider Electric as your turnkey solution partner we include in our solutions:
  - Project management and responsibility
  - Engineered systems
  - Third-party components management

We provide on-site services and support
- Qualified personnel to deliver on-site engineering and technical services

We improve your service team's competencies
- Service and commissioning training

Operate

We provide international sales and after-sales services for you and your customers
- Maintenance contracts
- Spares parts
- Repairs
- Normal and express deliveries
- Service expertise:
  - Error diagnosis and repair
  - Environmental measurements (EMC, field bus, thermography, power quality analyses, etc.)
- Customer International Support (CIS) as a single point of contact:
  - A network of 190 dedicated local country experts
  - A web-based collaborative platform for efficient communication

Improve

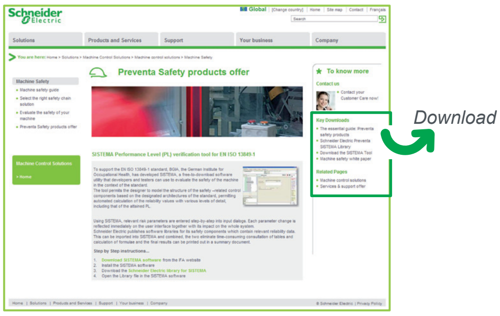
Improve your machine ranges
- Consulting

We improve your customer's machines in their production line
- Audits
- Retrofitting
- Migration and upgrade
- Training

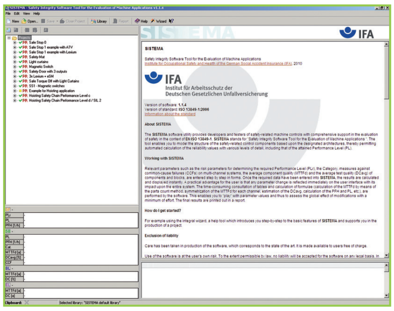
Safety Legislation and Standards

Service we provide

Schneider Electric Library for SISTEMA



Schneider Electric library for SISTEMA



SISTEMA software

To support the EN/ISO 13849-1 standard, IFA, the German Institute for Occupational Health, has developed SISTEMA, a free-to-download software utility that designers and verifiers can use to evaluate the safety of the machine in the context of the standard.

The tool permits the designer to model the structure of the safety-related control components based on the designated architectures of the standard, permitting automated calculation of the reliability values with various levels of detail, including that of the attained PL.

Using SISTEMA, relevant risk parameters are entered step-by-step into input dialogs. Each parameter change is reflected immediately on the user interface together with its impact on the whole system.

Schneider Electric publishes software libraries for its safety components which contain relevant reliability data. This can be imported into SISTEMA and combined, the two eliminate time-consuming consultation of tables and calculation of formulae and the final results can be printed out in a summary document.

Safety Legislation and Standards
Industrial accidents

Industrial accidents

An industrial accident occurs through work or in the workplace and causes minor to serious injury to a person using a machine, feeding it or carrying out special work on it (fitter, operator, maintenance personnel, etc.).

Causes of accidents in the workplace

- Human-related factors (designers, users):
  - poor grasp of machine design
  - over-familiarity with danger through habit and failure to take dangerous situations seriously
  - underestimation of hazards, causing people to ignore safe working procedure
  - loss of concentration on tasks to be performed (e.g. fatigue)
  - failure to comply with procedures
  - stressful working conditions (noise, work rates, etc.)
  - uncertainty of employment which can lead to inadequate training
  - inadequate or bad maintenance, generating unsuspected hazards
- Machine-related factors:
  - inadequate guards
  - inherent machine hazards (e.g. reciprocal motion of a machine, unexpected starting or stopping)
  - machines not suited to the application or environment (e.g. sound alarms deadened by the noise of surrounding machinery)
- Plant-related factors:
  - movement of personnel from machine to machine (automated production line)
  - machinery from different manufacturers and using different technologies
  - flow of materials or products between machines

Consequences

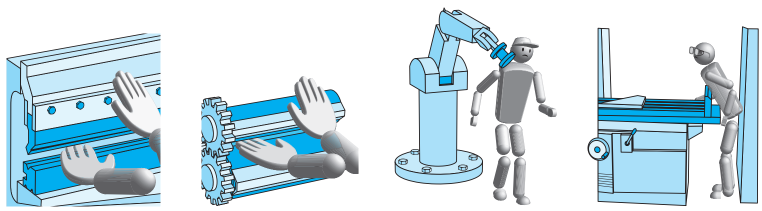
- Risk of varying degrees of physical injury to the user
- stoppage of the machine involved
- stoppage of similar machine installations for inspection, for example by health and safety inspectors
- if necessary, modifications to make machinery safe
- change of personnel and training new personnel for the job
- damage to the company brand image

Conclusion

Damages for physical injuries are equivalent to about 20 thousand million euro paid out each year in the European Union. Decisive action is required to reduce the number of accidents in the workplace. The first essentials are adequate company policies and efficient organisation.
Reducing the number of industrial accidents and injuries depends on the safety of machines and equipment.

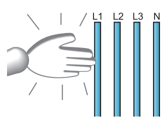
Types of potential hazard

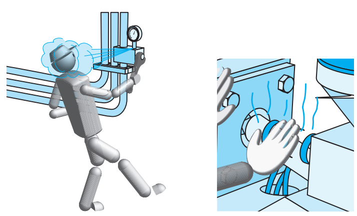
The potential hazards of a machine can be classified into three main groups, as illustrated below:



Mechanical hazards

Puncturing, cutting, shearing, fractures, severing	Catching, entanglement, drawing in, trapping	Impact	Crushing





Electrical hazards	**Physical and chemical hazards**	
Electric shock, electrocution, burns	*Discharge of dangerous substances*	*Burns*

Safety Legislation and Standards
European legislation

European legislation

Safety has become a key issue for businesses. Social developments in association with technological progress have had a profound impact on legislation and on regulations for the use of building electrical automation equipment.

Social issues

The safety-conscious nature of our western societies has led the legislature to increase the number of requirements and establish stricter rules, while the high cost of accidents has prompted companies to make efforts in the same direction.

Technological issues

Increasing levels of automation have led to new restrictions. In some case it is difficult, if not dangerous, to stop a machine suddenly and it is necessary to perform a safe shut down sequence before allowing personnel to enter into a production cell. The increasingly widespread use of electronics and software has required a different approach to the solutions adopted; empirical rules are no longer enough. Selection includes a reliability calculation to determine the behavior of the system. In this context, the specification and design phase are crucial. Studies show that more than 2/3rds of incidents are due to bad design and inadequate specifications. At this stage it is therefore necessary to estimate potential risks and select the most appropriate solutions to reduce their consequences. Standards are available to assist and guide the designer.

Manufacturers of components and solutions help their customers by offering complete, ready-to-use functions which, when combined in accordance with the regulations, satisfy the customer’s needs and meet legislative requirements. In this chapter, we will present a simplified process. To make a choice, the customer will then be able to refer to the safety functions chapter and to the safety products chapters.

European legislation requires that preventive action be taken to preserve and protect the quality of the environment and human health. To achieve these objectives, European Directives have been prepared which must be applied by plant operators and by manufacturers of equipment and machines. It also assigns responsibility for possible accidents.

- Notwithstanding the constraints, machine safety has the following positive repercussions:
  - prevention of industrial accidents
  - protection of workers and personnel by means of suitable safety measures that take into account the machine’s application and the local environment
- This makes it possible to reduce direct and indirect related costs:
  - by reducing physical harm
  - by reducing insurance premiums
  - by reducing production losses and possible delay penalties
  - by limiting damages and costs for maintenance
- Safe operation involves two principles: safety and reliability of the process:
  - safety is the ability of a device to keep the risk incurred by persons within acceptable limits
  - reliability of operation is the ability of a system or device to perform its function at any moment in time and for a specified duration
- Safety must be taken into account right from the beginning of the design stage and kept in place throughout all stages of a machine’s life cycle: transport, installation, commissioning, maintenance, dismantling

The main purpose of the Machinery Directive 2006/42/EC is to compel manufacturers to guarantee a minimum safety level for machinery and equipment sold within the European Union. This version has been replacing the 98/37/EC version since January 2010.

To allow free circulation of machinery within the European Union, the CE marking must be applied to the machine and an EC declaration of conformity is issued to the purchaser. This directive came into effect in January 1995 and has been enforced since January 1997 for all machines.

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

These standards are complex. After a brief presentation of the structure of the standards system, we will provide the practical guide to the typical standards to be applied according to the selected control system design.

Safety Legislation and Standards
Certification and CE marking

Certification and CE marking

There are 6 stages in the process for certification and affixing of the CE marking on machines:
1 Apply all the relevant directives
2 Conform to the essential health and safety requirements
3 Draw up the technical documentation
4 If applicable proceed with the conformity examination
5 Draw up the Declaration of Conformity
6 Affix the CE marking

The Machinery Directive

The Machinery Directive is an example of the “New approach” for the harmonization of products in terms of technical specifications and standards.
It is based on:
> Essential health and safety requirements which must be complied with before the machine is put on the market
> A voluntary harmonization process of standards undertaken by the European Standards Committee (CEN) and the European committee for electro-technical standardization (CENELEC)
> Conformity of evaluation procedures adapted to the types of risk and associated with machine types
> The CE marking, affixed by the manufacturer to indicate that the machine conforms to the applicable directives; machines bearing this marking can circulate freely within the European Union

The directive has considerably simplified the multiple national legislations which were in force and has therefore removed many barriers which made trading difficult in the European Union. This has also made it possible to reduce the social cost of accidents. The directives do not apply to pre-existing machines within the EU unless they are substantially modified. A list of the machines requiring special attestation procedures can be found in the Machinery Directive Annex 4.

The essential requirements

Annexe I of the Machinery Directive groups together the essential health and safety requirements, for putting machines and safety components on the market and into service in Europe.

It follows that:
> If all the requirements of the directive are complied with, no member state of the European Union can oppose circulation of this product
> If the requirements of the directive are not complied with, putting the product on the market may be prohibited or withdrawal of the product from the market may be required

In the European Union, this concerns not only manufacturers or their distributors, but also importers and resellers who import these machines or put them into service. Second-hand machines within the EU are not covered, but used machines that have been modified or refurbished can be considered to be new machines.

The harmonized standards

The simplest way to demonstrate conformity with the directives is to conform to the European Harmonized Standards. When, for a product listed in Annex 4 of the Machinery Directive, there is no harmonized standard, or the existing standards are not relevant to cover the essential health and safety requirements, or if the manufacturer considers that these standards are not applicable to their product, they can apply for approval by an outside Notified Body.

These bodies are approved by the Member States after having shown that they have the recognized expertise to give such an opinion (TÜV, BGIA, INRS, BSI Product Services, etc.).

Although the Notified Body has a certain number of responsibilities under the Directive, it is always the manufacturer or their representative who remain responsible for conformity of the product.

Certification and CE marking

Declaration of conformity

In accordance with Article 1 of the Machinery Directive, the manufacturer or their authorized representative established in the European Union must draw up a European Declaration of Conformity for each machine (or safety component). This is in order to certify that the machine or safety component conforms to the Directive.

Before putting a product on the market, the manufacturer or their representative must prepare a technical file.

CE marking

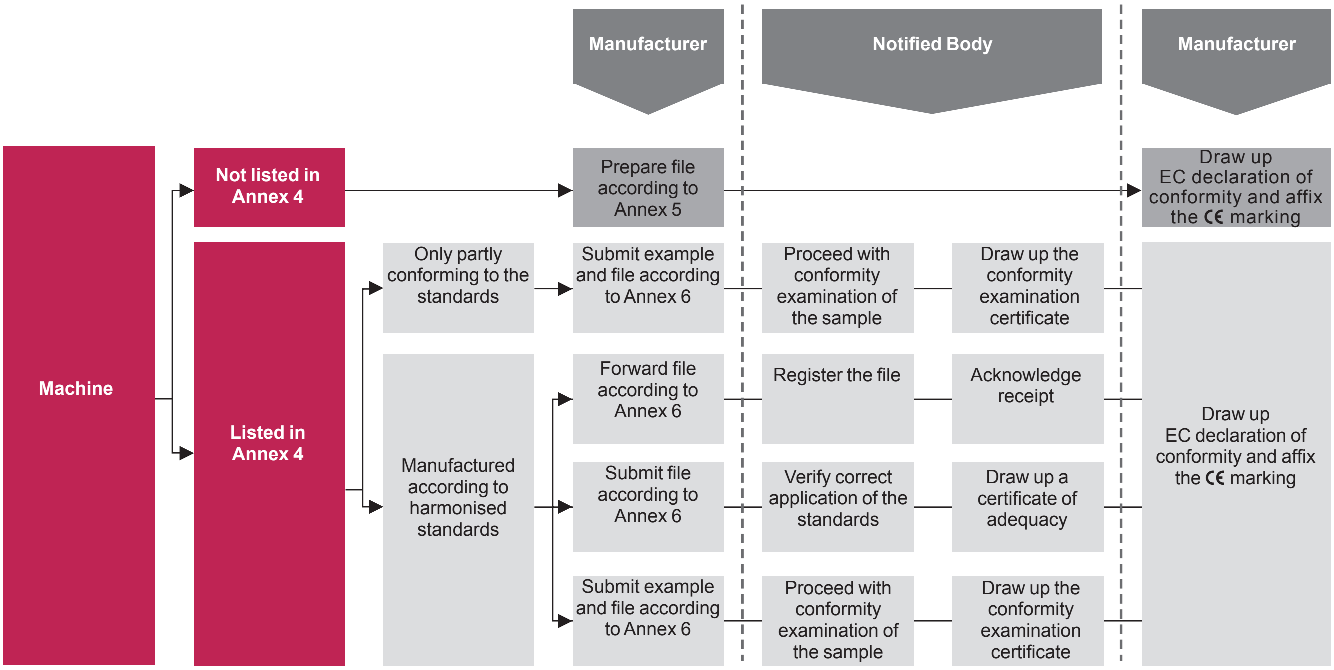
Finally, the CE mark must be affixed to the machine by the manufacturer or their authorized representative in the European Union. This marking has been obligatory since 1st January 1995 and can only be affixed if the machine conforms to all the applicable directives, such as:

- The Machinery Directive 2006/42/ECC
- The Electromagnetic Compatibility (EMC) directive 2004/108/EC
- The Low Voltage Directive 2006/95/EC

There are other directives such as the protection of persons, lifts, medical equipment, etc., which may also be applicable.

The CE marking is the machine's passport in the European Union, which allows it to be marketed in all countries within the Union without taking into account regulations in each individual country.

CE marking procedure



Safety Legislation and Standards
Standards

Standards

Introduction

The harmonized European safety standards establish technical specifications which comply with the minimum safety requirements defined in the related directives. Compliance with all applicable harmonized European standards can be assumed to ensure compliance with the related directives. The main purpose is to guarantee a minimum safety level for machinery and equipment sold within the EU market and allow the free circulation of machinery within the European Union.

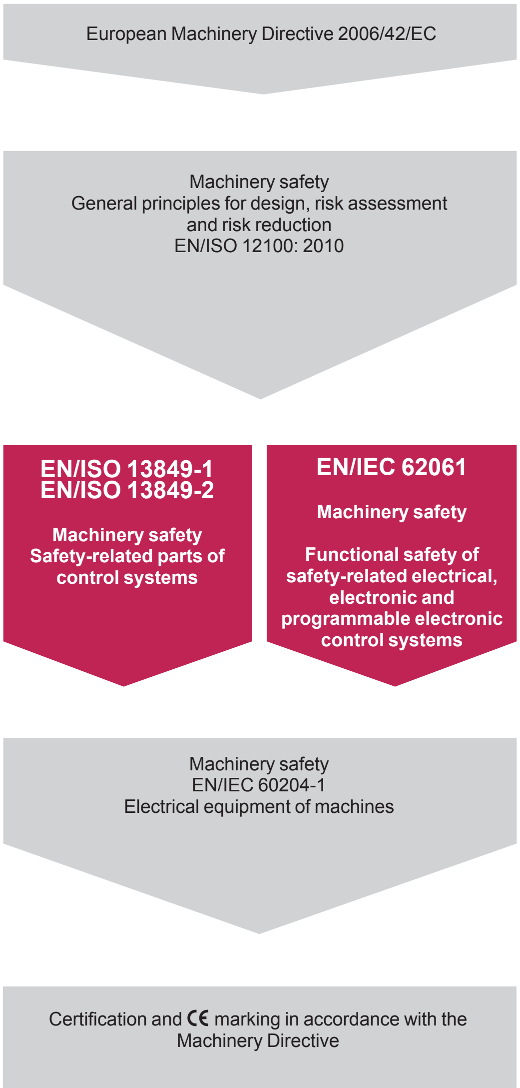
The 3 groups of European standards

- Type **A** standards
  Basic safety standards which specify the basic concepts, design principles and general aspects valid for all types of machine: e.g. EN/ISO 12100
- Type **B** standards
  Standards relating to specific aspects of safety or to a particular device that can be used on a wide range of machines
- Type **B1** standards
  Standards relating to specific safety aspects of machines: e.g. EN/IEC 60204-1 Electrical equipment of machines
- Type **B2** standards
  Standards relating to specific products such as two-hand control stations (EN 574), guard switches (EN 1088/ISO 14119), emergency stops (EN/ISO 13850), etc
- Type **C** standards
  Standards relating to various families or groups of machines (e.g.: hydraulic presses EN 693, robots, etc) and giving detailed applicable requirements

A selection of standards

Standards	Type	Subject
EN/ISO 12100	A	Machinery safety - General principles for design, risk assessment and risk reduction
EN 574	B	Two-hand control devices - Functional aspects and design principles
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	Machinery safety - Safety-related parts of control systems - Part 1 General principles for design
EN/ISO 13849-2	B	Machinery safety - Safety-related parts of control systems - Part 2 Validation
EN 349	B	Minimum gaps to avoid crushing parts of the human body
EN 294	B	Safety distances to prevent hazardous zones being reached by upper limbs
EN 811	B	Safety distances to prevent hazardous zones being reached by lower limbs
EN/IEC 60204-1	B	Machinery safety - Electrical equipment of machines - Part 1: general requirements
EN 999/ISO 13855	B	Positioning of protective equipment in respect of approach speeds of body parts
EN 1088/ISO 14119	B	Interlocking devices associated with guards - Principles for design and selection
EN/IEC 61496-1	B	Electro-sensitive protective equipment
EN/IEC 60947-5-1	B	Electromechanical control circuit devices
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/IEC 61800-5-2	B	Adjustable speed electrical power drive systems. Part 5-2: Safety requirements – Functional
EN 201	C	Machinery for plastics and rubber - Injection moulding machines – Safety requirements
EN 692	C	Mechanical presses - Safety requirements
EN 693	C	Hydraulic presses - Safety requirements
EN 289	C	Machinery for plastics and rubber - Presses - Safety requirements
EN 422	C	Blow moulding machines for producing hollow parts - Design and construction requirements
EN/ISO 10218-1	C	Manipulating industrial robots - Safety requirements
EN 415-4	C	Safety of packaging machines - Part 4: palletisers and depalletisers
EN 619	C	Safety and EMC requirements for equipment for mechanical handling of unit loads
EN 620	C	Safety and EMC requirements for fixed belt conveyors for bulk material
EN 746-3	C	Industrial thermo processing equipment - Part 3: safety requirements for the generation and use of atmosphere gases

Standards to be applied



Standards to be applied for the design of machines

The process

European Machinery Directive 2006/42/EC
Compliance with the following standards ensure compliance with the Machinery Directive (this new version of the Machinery Directive 2006/42/EC has been replacing 98/37/EC since January 2010).

EN/ISO 12100: 2010: General principles for design, risk assessment and risk reduction.
The purpose of this standard is to provide designers with an overall framework and guidance to enable them to produce machines that are safe for their intended use.

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

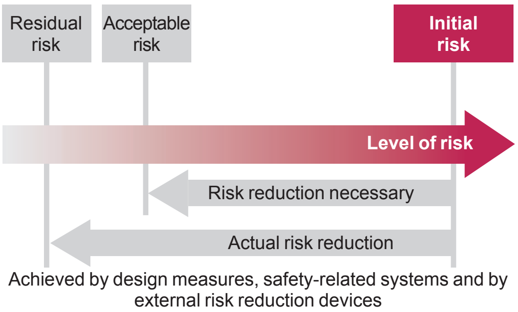
Remarks:
The use of either the EN/ISO 13849 or EN/IEC 62061 standards gives presumption of conformity to the new 2006/42/EC directive.

EN/IEC 60204-1: Electrical equipment of machines
Standard EN/IEC 60204-1 completes the safety standards by giving setting-up rules for each component of a machine’s electrical functions.
It specifies, amongst other things:
- the type of connection terminals and disconnection and breaking devices
- the type of electric shock protection
- the type of control circuits
- the type of conductors and wiring rules
- the type of motor protection

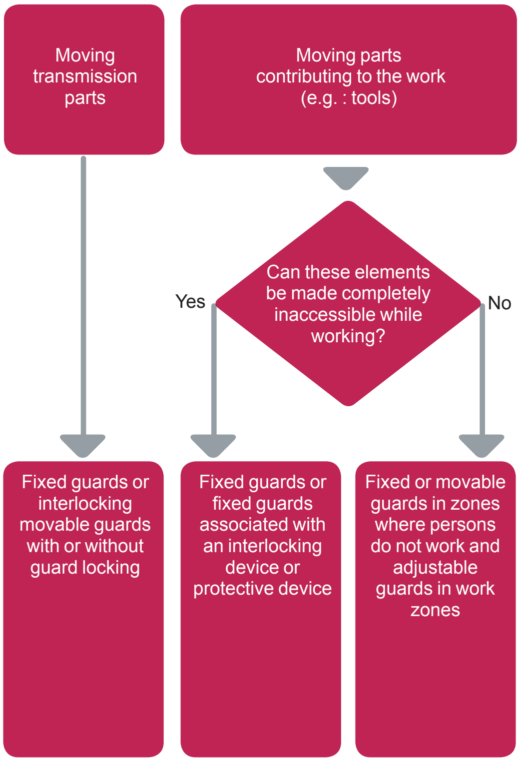
Standard to be applied according to the design selected for the safety related machine control system

Safety standards to be applied according to type of architecture selected
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

Risk and safety



Reduction of risk to an acceptable level



Selection of the protection system (EN/ISO 12100: 2010)

Safety is the absence of risks which could cause injury to or damage the health of persons. Functional safety is a part of safety that depends on the correct operation of safety functions.

According to the requirements of standard EN/ISO 12100: 2010, the machine designer's job is to reduce all risks to a value lower than the acceptable risk. For more details concerning the sources of accidents and risk prevention, the reader is referred on page 6.

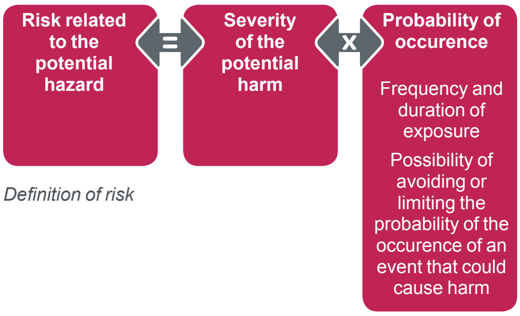
This standard recognizes two sources of hazardous phenomena:
> Moving transmission parts
> Moving parts contributing to the work

It gives guidelines for the selection and installation of devices which can be used to protect persons and identifies those measures that are implemented by the machine designer and those dependent on its user.

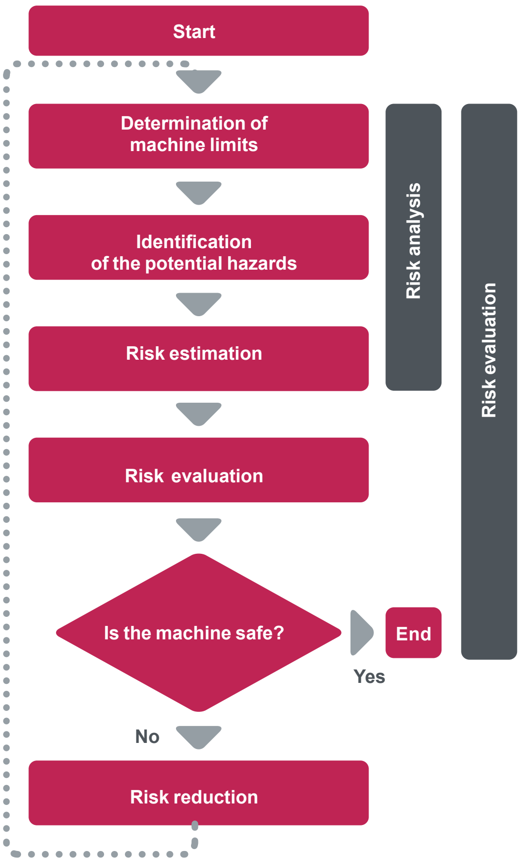
The measures taken by the machine designer may be:
> Inherent in the design
> Selection of guards and additional measures, including control systems
> Information for the user

The measures taken by the user may be (non-exhaustive list):
> Organization, procedures, etc.
> Personal protective equipment
> Training

Risk Assessment



Definition of risk



Logic steps for risk analysis

Assessment of machinery related risk

European legislation

Machines are sources of potential risk and the Machinery Directive requires a risk assessment to ensure that any potential risk is reduced to less than the acceptable risk.

Standard EN/ISO 12100 defines risk as follows: risk is the severity multiplied by the possibility of occurrence. It defines an iterative process for achieving machine safety, which states that the risks for each potential hazard can be determined in four stages. This method provides the basis for the requisite risk reduction.

Risk assessment

> Risk assessment consists of a series of logic steps which make it possible to systematically analyze and evaluate machinery-related risks
> Risk assessment is followed, whenever necessary, by a reduction of the risk. This definition taken from standard EN/ISO 12100 is based on an iterative process represented in the diagram opposite

Determination of machine limits

Risk assessment starts by determining the limits of the machine at all stages of its life cycle:

> Transport, assembly, installation
> Commissioning
> Use
> De-commissioning, dismantling

The use limitations must then be specified:

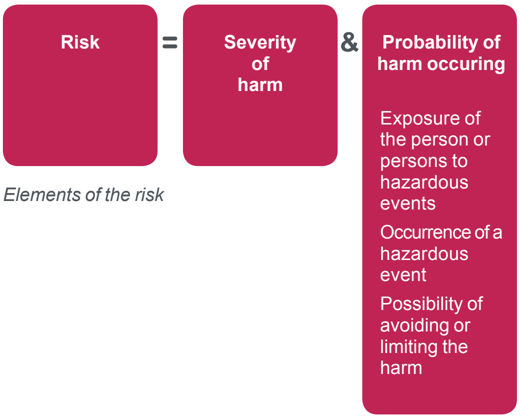
> Operating modes
> Level of training required
> Space limits (amplitude, movement)
> Time limits (life cycle, frequency of maintenance)

Identification of the potential hazard

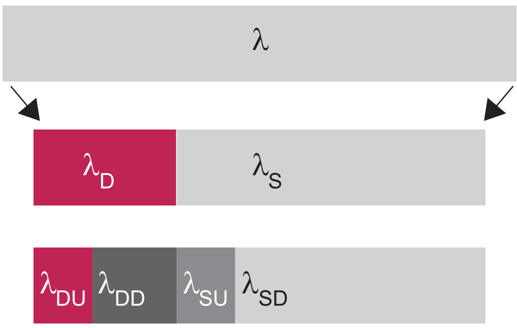
If a potential hazard exists, a hazardous phenomenon will cause harm if measures are not taken.
All the tasks associated with the machine's life cycle must be identified, such as:

> Assembly, transport and installation
> Adjustment, testing
> Learning, programming
> Tool changing
> Feeding, removal of product from the machine
> Starting, stopping
> Emergency Stops, restarting after an unexpected stop
> Maintenance, cleaning, etc.

Risk Assessment



Elements of the risk



λ rate of control system failures
λ_D rate of dangerous failures
λ_{DU} rate of undetected dangerous failures
λ_{DD} rate of detected dangerous failures
λ_S rate of safe failures
λ_{SU} rate of undetected safe failures
λ_{SD} rate of detected safe failures

Breakdown of the probability of failures

Risk estimation

The risk is a function of the severity of the harm and the probability that this harm will occur.

> The severity of the harm takes into account:
  > The severity of injuries (slight, serious, death)
  > The extent of the harm (number of persons)

> The probability of the harm occurring takes into account:
  > Exposure to the hazard (nature of access, time spent in the hazardous zone, number of persons exposed, frequency of access, etc.)
  > The occurrence of a hazardous event (accident history, comparison of risks, etc.)
  > The possibility of avoiding or limiting the harm (experience, awareness of the risk, etc.)

Risk assessment

On the basis of the risk assessment, the designer has to define the safety related control system.
To achieve that, the designer will choose one of the two standards appropriate to the application:

> either standard EN/ISO 13849-1, which defines performance levels (PL)
> or standard EN/IEC 62061, which defines safety integrity level (SIL)

Risk reduction

The process of risk reduction for dangerous events starts by:

> Intrinsic prevention (inherently safe design)
> Definition of the appropriate protective means (guards, carters, fix fences, etc.)
> Personal training

If the selected preventive measure depends on a safety related control system, the designer has to perform an iterative process for the design of the safety relative control system.

> The first stage is to define the necessary safety-related control functions:
  > either through the choice of components
  > or by adapting the control system architecture. Redundancy (double circuit components), for example, significantly increases the reliability of the solution
> Once the limits of available technologies have been reached, it will not be possible to further reduce the rate of dangerous failures. To achieve the required level of safety, it will be necessary to use a diagnostic system that allows dangerous failures to be detected

Safety Legislation and Standards
How to choose between EN/ISO 13849 and EN/ IEC 62061

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	$\geqslant 10^{-5} \dots < 10^{-4}$
b	1	$\geqslant 3 \times 10^{-6} \dots < 10^{-5}$
c	1	$\geqslant 10^{-6} \dots < 3 \times 10^{-6}$
d	2	$\geqslant 10^{-7} \dots < 10^{-6}$
e	3	$\geqslant 10^{-8} \dots < 10^{-7}$

Recommended application of IEC 62061 and ISO 13849-1			
Annex	Technology implementing the safety related control fuction (S)	ISO 13849-1	IEC 62061
A	Non electrical, e.g. hydralics	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.

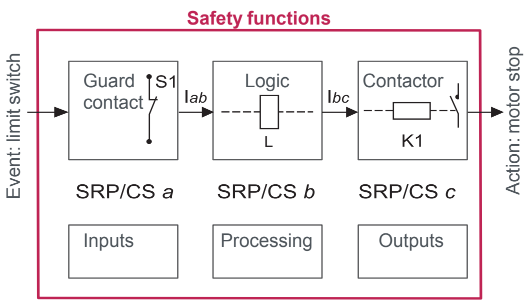
Note 1 Designated architecture are defined in Annex B of EN/ISO 13849-1 to give a simplified approach for qualification of performance level

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

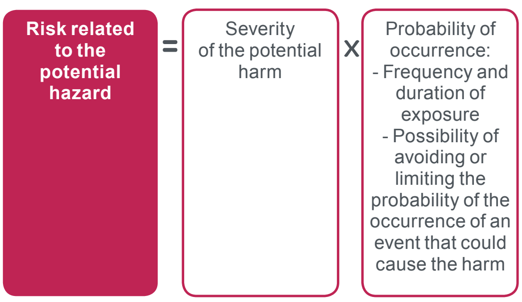
Note 3 For non-electrical technology use parts according to EN/ISO 13849-1 as subsystems.

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



Representation of the safety function



Risk analysis

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/CS*a*)
- The control logic, limited in this example to opening or closing of a contactor coil (SRP/CS*b*)
- The power output that controls the motor (SRP/CS*c*)
- The connections (I*ab*, I*bc*)

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

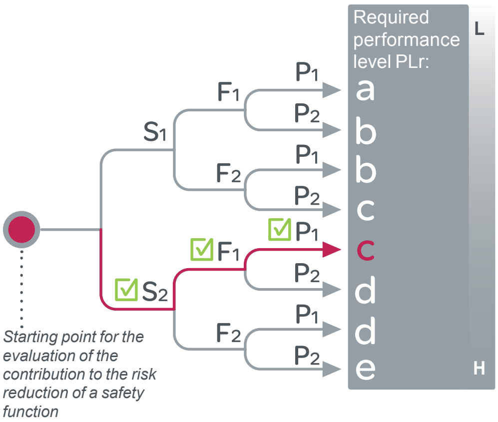
Standard EN/ISO 13849-1
Machinery safety - Safety-related parts of control systems *(continued)*

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.



Estimation of required performance level

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 to 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

L = Low contribution to risk reduction
H = High contribution to risk reduction
→ Estimation

Stage 3 - Design and creation of the safety functions

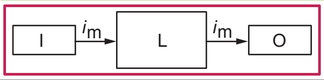
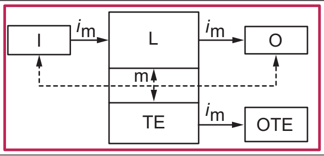
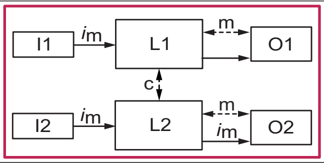
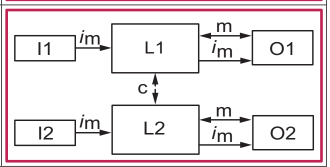
At this point, we need to describe the PL calculation method.

For a SRP/CS (or a combination of SRP/CS), PL could be estimated with the figure shown on page 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 occurence 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:
*i*m: 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)*

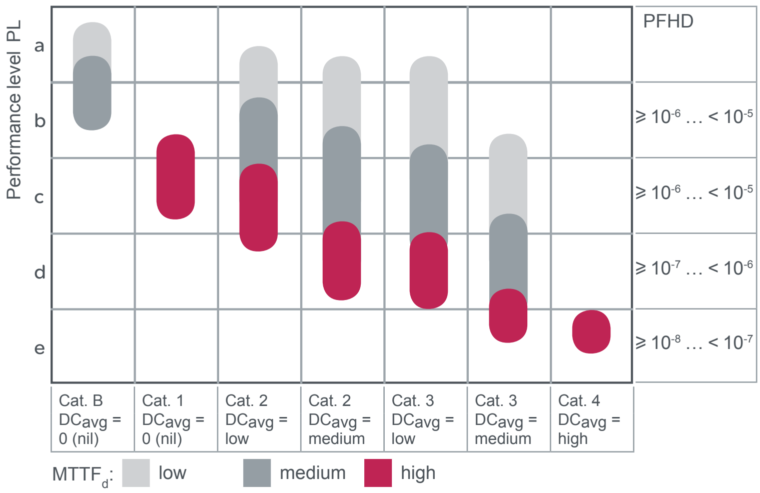
Stage 3- *(continued)*

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

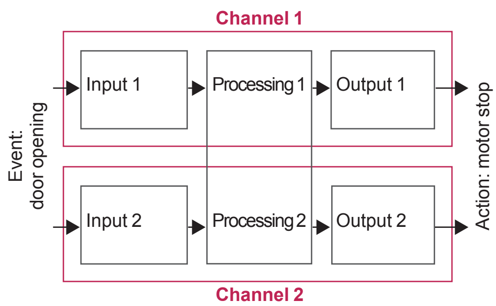
For example, in the event of welding of a N/C contact in a relay, the state of the N/O contact could incorrectly indicate the opening of the circuit, unless the relay has mechanically linked N/O and N/C contacts, when the fault can be detected.
The standard recognises four levels:

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 19)



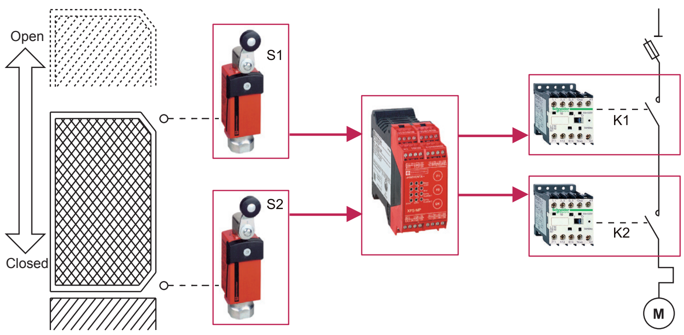
Functional diagram of the example

> 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.



Application scheme of the example

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 x 8 x (3600 / 90) = 70 400 operations/year
$MTTF_d = B_{10d} / (0.1 \times N)$ and $B_{10d} = B_{10}$ / % dangerous failure.

For the safety switches,
the $MTTF_d$= (1 / 0.20 x 10 000 000) / (0.1) x 70 400 = 7102 years
For the contactors,
the $MTTF_d$ = (1 / 0.73 x 1 000 000) / (0.1) x 70 400 = 194 years
The $MTTF_d$ for each channel will then be calculated using the formula:

$$\frac{1}{MTTF_d} = \frac{1}{MTTF_{da}} + \frac{1}{MTTF_{db}} + \frac{1}{MTTF_{dc}}$$

i.e. 85 years for each channel.
A similar formula is used to calculate the diagnostic capability

$$DC_{avg} = \frac{\frac{DC_a}{MTTF_{da}} + \frac{DC_b}{MTTF_{db}} + \frac{DC_c}{MTTF_{dc}}}{\frac{1}{MTTF_{da}} + \frac{1}{MTTF_{db}} + \frac{1}{MTTF_{dc}}}$$

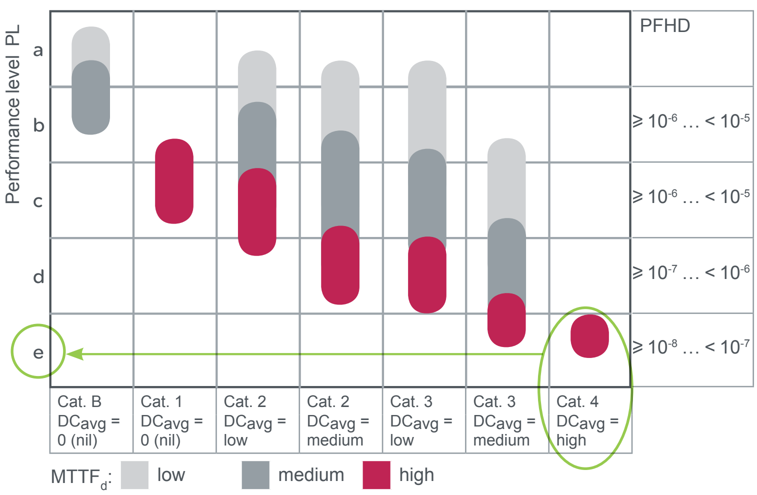
The result of the calculation in our example gives a value of 99%

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.

Safety Legislation and Standards
Standard EN/IEC 62061

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.

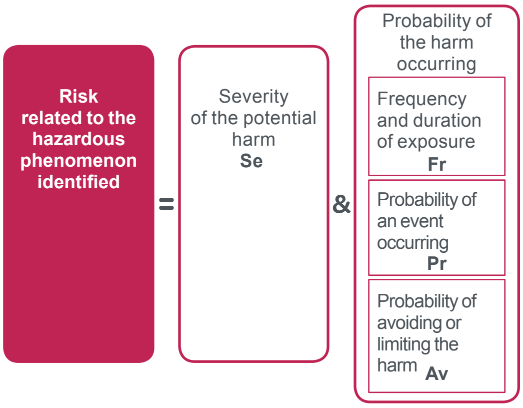
A particular feature of this standard is that it prompts the user to make a functional analysis of the architecture, then split it into sub-functions and analyse their interactions before deciding on a hardware solution for them (the SRECS).

> 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

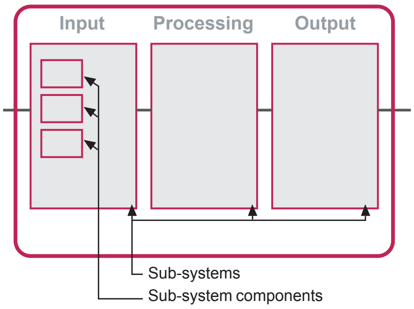
> Functional safety

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 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 dangerous component (cutting, temperature, electrical) and the possibility for a person to identify a hazardous phenomenon.

Probability of avoiding or limiting the harm	Av
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:

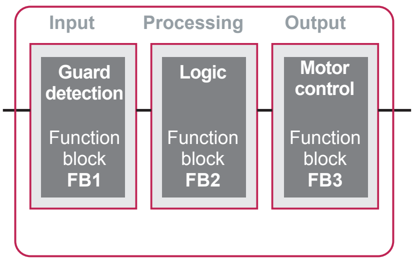
- Fr = 5 accessed several times a day
- Pr = 4 hazardous event probable
- Av = 3 probability of avoiding almost impossible

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

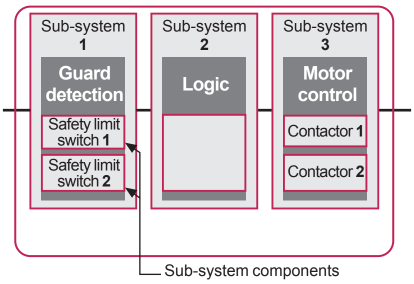
Se	Class CI				
	3-4	5-7	8-10	11-13	14-15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3	-	-	SIL 1	SIL 2	SIL 3
2	-	-	-	SIL 1	SIL 2
1	-	-	-	-	SIL 1

SRECS
Objective SIL 2



***Stage 2**: Break down into function blocks*

SRECS



***Stage 3**: Assignment of function blocks*

> Basic structure of the **SRECS**

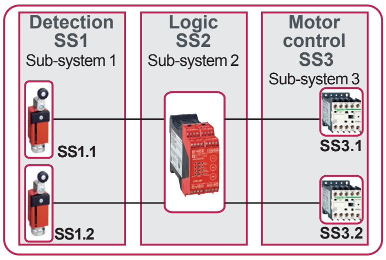
Without going into detail about the hardware components to be used, the system is broken down into sub-systems. In our case, we find the 3 sub-systems that will perform the input, processing and output functions. The figure opposite illustrates this stage, using the terminology given in the standard.

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

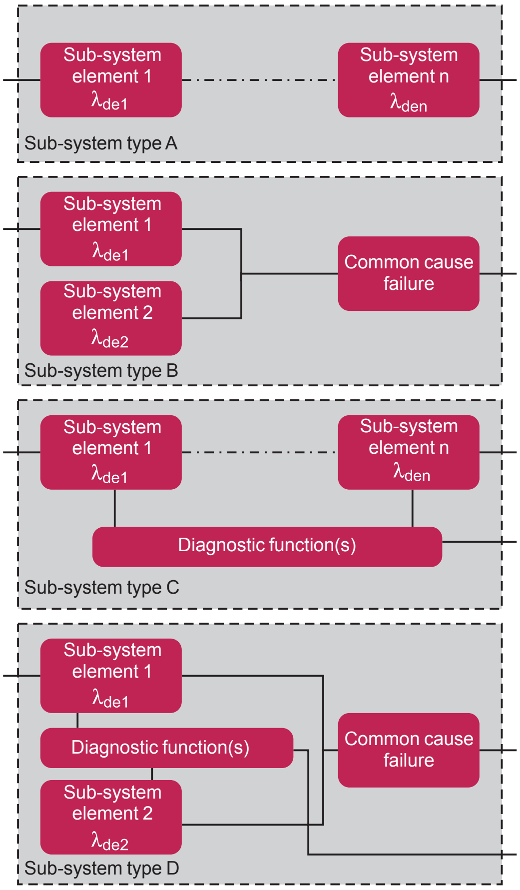
A function block (**FB**) is the result of a detailed break down of a safety-related function.
The function block structure gives an initial concept of the SRECS architecture.
The safety requirements of each block are deduced from the specification of the safety requirements of the system's function.

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

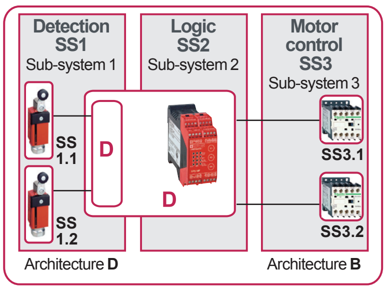
Each function block is assigned to a sub-system in the SRECS architecture. A failure of any sub-system will lead to the failure of the safety-related control function. More than one function block may be assigned to each sub-system. Each sub-system may include sub-system elements and, if necessary, diagnostic 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.



***Stage 4**: Component selection*



Types of sub-system architecture



***Stage 5**: Design of the diagnostic function*

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

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:
- $\mathbf{B_{10}}$: number of operations at which 10% of the population fail
- **C**: Duty cycle (number of operations per hour)
- λ_D: rate of dangerous failures ($\lambda_D = \lambda$ x 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 $PFH_d = 1.6\ E^{-9}$
- for SS3 $PFH_d = 1.06\ E^{-7}$

The total probability of dangerous failures per hour is:
- $\mathbf{PFH_{DSRECS} = PFH_{DSS1} + PFH_{DSS2} + PFH_{DSS3}}$
- $\mathbf{PFH_{DSRECS}} = 1.6\ 10^{-9} + 7{,}38\ 10^{-9} + 1.06\ E^{-7} = 1.15\ E^{-7}$

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	$\geq 10^{-8}$ ... $< 10^{-7}$
2	$\mathbf{\geq 10^{-7}}$ **...** $\mathbf{< 10^{-6}}$
1	$\geq 10^{-6}$ ... $< 10^{-5}$

More information on
http://www.schneider-electric.com/machinesafety

Schneider Electric Industries SAS

www.schneider-electric.com

Head Office
35, rue Joseph Monier
F-92500 Rueil-Malmaison
France

Design: Schneider Electric
Photos: Schneider Electric

DIA3ED2150103EN

01/2015